

SIP Speaker with Talk-Back Operations Guide

Part #011394

Document Part #932005C
for Firmware Version 20.5.0

CyberData Corporation
3 Justin Court
Monterey, CA 93940
(831) 373-2601

SIP Speaker Operations Guide 932005C
Part # 011394

COPYRIGHT NOTICE:

© 2023, CyberData Corporation, ALL RIGHTS RESERVED.

This manual and related materials are the copyrighted property of CyberData Corporation. No part of this manual or related materials may be reproduced or transmitted, in any form or by any means (except for internal use by licensed customers), without prior express written permission of CyberData Corporation. This manual, and the products, software, firmware, and/or hardware described in this manual are the property of CyberData Corporation, provided under the terms of an agreement between CyberData Corporation and recipient of this manual, and their use is subject to that agreement and its terms.

DISCLAIMER: Except as expressly and specifically stated in a written agreement executed by CyberData Corporation, CyberData Corporation makes no representation or warranty, express or implied, including any warranty or merchantability or fitness for any purpose, with respect to this manual or the products, software, firmware, and/or hardware described herein, and CyberData Corporation assumes no liability for damages or claims resulting from any use of this manual or such products, software, firmware, and/or hardware. CyberData Corporation reserves the right to make changes, without notice, to this manual and to any such product, software, firmware, and/or hardware.

OPEN SOURCE STATEMENT: Certain software components included in CyberData products are subject to the GNU General Public License (GPL) and Lesser GNU General Public License (LGPL) “open source” or “free software” licenses. Some of this Open Source Software may be owned by third parties. Open Source Software is not subject to the terms and conditions of the CyberData COPYRIGHT NOTICE or software licenses. Your right to copy, modify, and distribute any Open Source Software is determined by the terms of the GPL, LGPL, or third party, according to who licenses that software.

Software or firmware developed by CyberData that is unrelated to Open Source Software is copyrighted by CyberData, subject to the terms of CyberData licenses, and may not be copied, modified, reverse-engineered, or otherwise altered without explicit written permission from CyberData Corporation.

TRADEMARK NOTICE: CyberData Corporation and the CyberData Corporation logos are trademarks of CyberData Corporation. Other product names, trademarks, and service marks may be the trademarks or registered trademarks of their respective owners.



Technical Support

The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:
<https://support.cyberdata.net/>

Phone: (831) 373-2601, Ext. 333

Email: support@cyberdata.net

Fax: (831) 373-4193



Company and product information is at www.cyberdata.net.

Revision Information

Revision 932005C, which corresponds to firmware version 20.5.0, was released on December 11, 2023, and has the following changes:

- Updates [Figure A-1, "Ceiling Tile Mounting"](#)
- Updates [Figure A-2, "Drywall Mounting"](#)

Pictorial Alert Icons

	<p>General Alert</p> <p><i>This pictorial alert indicates a potentially hazardous situation. This alert will be followed by a hazard level heading and more specific information about the hazard.</i></p>
	<p>Ground</p> <p><i>This pictorial alert indicates the Earth grounding connection point.</i></p>

Hazard Levels

Danger: Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury. This is limited to the most extreme situations.

Warning: Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.

Caution: Indicates a potentially hazardous situation which, if not avoided, could result in minor or moderate injury. It may also alert users against unsafe practices.




Notice: Indicates a statement of company policy (that is, a safety policy or protection of property).

The safety guidelines for the equipment in this manual do not purport to address all the safety issues of the equipment. It is the responsibility of the user to establish appropriate safety, ergonomic, and health practices and determine the applicability of regulatory limitations prior to use. Potential safety hazards are identified in this manual through the use of words Danger, Warning, and Caution, the specific hazard type, and pictorial alert icons.

Important Safety Instructions

1. Read these instructions.
2. Keep these instructions.
3. Heed all warnings.
4. Follow all instructions.
5. Do not use this apparatus near water.
6. Clean only with dry cloth.
7. Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.
8. Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
9. Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
10. Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
11. Only use attachments/accessories specified by the manufacturer.
12. Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.
13. Prior to installation, consult local building and electrical code requirements.

14. WARNING: The SIP Speaker with Talk-Back enclosure is not rated for any AC voltages!

 GENERAL ALERT	Warning <i>Electrical Hazard:</i> This product should be installed by a licensed electrician according to all local electrical and building codes.
 GENERAL ALERT	Warning <i>Electrical Hazard:</i> To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.
 GENERAL ALERT	Warning The PoE connector is intended for intra-building connections only and does not route to the outside plant.

Abbreviations and Terms

Abbreviation or Term	Definition
A-law	A standard companding algorithm, used in European digital communications systems to optimize, i.e., modify, the dynamic range of an analog signal for digitizing.
AVP	Audio Video Profile
Cat 5	TIA/EIA-568-B Category 5
DHCP	Dynamic Host Configuration Protocol
LAN	Local Area Network
LED	Light Emitting Diode
Mbps	Megabits per Second.
NTP	Network Time Protocol
PBX	Private Branch Exchange
PoE	Power over Ethernet (as per IEEE 802.3af standard)
RTFM	Reset Test Function Management
SIP	Session Initiated Protocol
SRTP	Secure Real Time Protocol
u-law	A companding algorithm, primarily used in the digital telecommunication
UC	Unified Communications
VoIP	Voice over Internet Protocol

Contents

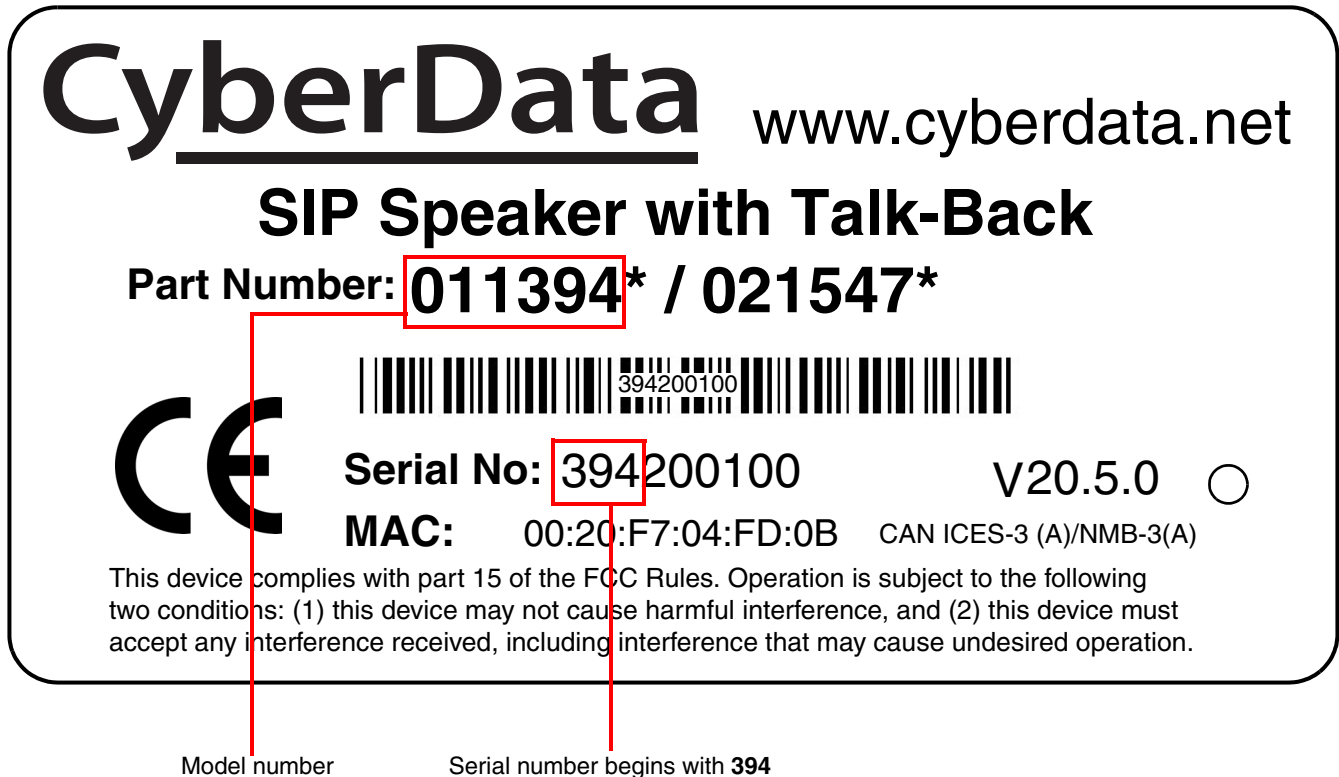
Chapter 1 Product Overview	1
1.1 How to Identify This Product	1
1.2 Installation	2
1.3 Features	3
1.4 Supported Protocols	4
1.5 Supported SIP Servers	4
1.6 Specifications	5
1.7 Optional Connections	6
1.8 Compliance	7
1.8.1 CE Statement	7
1.8.2 FCC Statement	7
1.8.3 Industry Canada (IC) Compliance Statement	7
 Chapter 2 Installing the SIP Speaker with Talk-Back	 8
2.1 Parts List	8
2.2 Device Configuration	9
2.2.1 Connect Power to the Speaker	10
2.2.2 Installation Options	12
2.2.3 Confirm that the Speaker is Operational and Linked to the Network	16
2.2.4 Confirm the IP Address and Test the Audio	17
2.2.5 How to Set the Factory Default Settings	18
2.3.1 Factory Default Settings	19
2.3.2 SIP Speaker with Talk-Back Web Page Navigation	20
2.3.3 Using the Toggle Help Button	21
2.3.4 Log in to the Configuration Home Page	23
2.3.5 Configure the Device	27
2.3.6 Configure the Audio	31
2.3.7 Configure the Network Parameters	35
2.3.8 Configure the SIP (Session Initiation Protocol) Parameters	38
2.3.9 Configure the SSL Parameters	48
2.3.10 Configure the Multicast Parameters	54
2.3.11 Configure the Sensor Configuration Parameters	57
2.3.12 Configure the Audiofiles Page Parameters	62
2.3.13 Configure the Events Parameters	68
2.3.14 Configure the Autoprovisioning Parameters	73
2.4.1 Downloading the Firmware	84
2.4.2 Reboot the Device	87
2.5.1 Command Interface Post Commands	88
 Appendix A Mounting the Speaker	 89
A.1 Ceiling Tile Mounting	89
A.2 Drywall Mounting	92
A.3 Dimensions	93
 Appendix B Troubleshooting/Technical Support	 94
B.1 Frequently Asked Questions (FAQ)	94
B.2 Documentation	94
B.3 Contact Information	95
B.4 Warranty and RMA Information	95
 Index	 96

1 Product Overview

1.1 How to Identify This Product

To identify the SIP Speaker with Talk-Back, look for a model number label similar to the one shown in [Figure 1-1](#). The model number on the label should be **011394**.

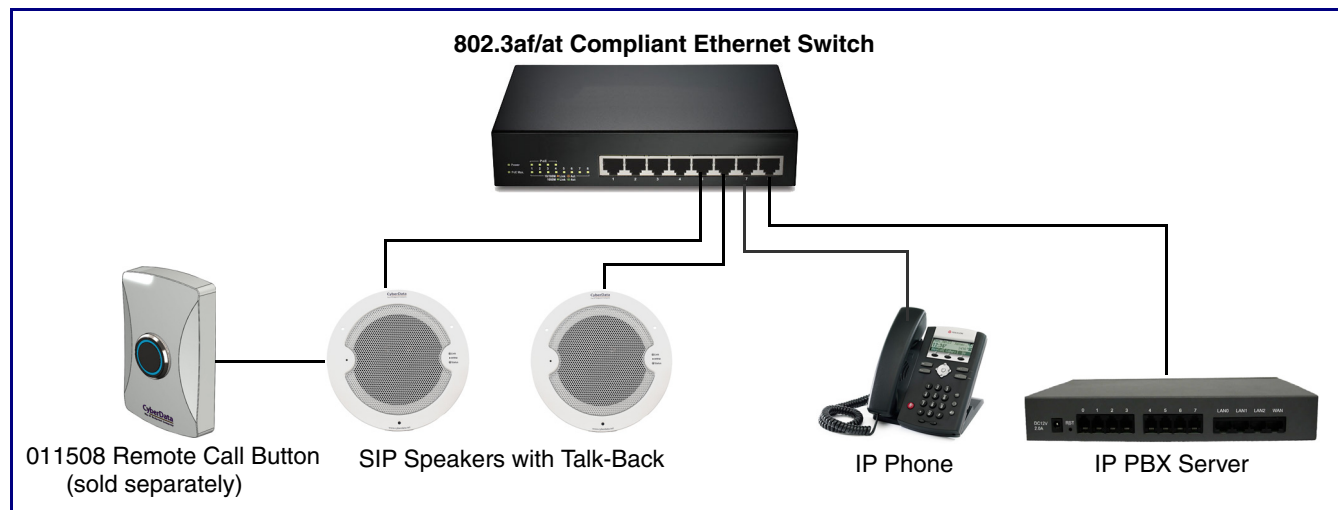
Figure 1-1. Model Number Label



1.2 Installation

Figure 1-2 illustrates a typical configurations for the SIP Speaker with Talk-Back.

Figure 1-2. Typical Installation



See the following sections for other installation options:

- [Section 2.2.2.2, "SIP Speaker with Talk-Back with an External Device"](#)
- [Section 2.2.2.3, "SIP Speaker with Talk-Back with Auxiliary Speaker Connection"](#)
- [Section 2.2.2.4, "SIP Speaker with Talk-Back with Line Out"](#)

1.3 Features

- Talk-back capability can be enabled during provisioning or from the web page
 - Full duplex audio with configurable echo cancelling
 - Adaptive half duplex audio with configurable VOX (Voice-Operated Switch) settings
 - Half duplex push to talk audio from the far side using the phone's keypad or from the Speaker side using CyberData's Remote Call Button
 - Ambient noise compensation, where the device will measure the ambient sound level in the area and adjust the volume of the speaker accordingly
 - Audio health check to verify hardware functionality that can be scheduled or launched manually
 - Configurable event generation for device health and status monitoring
 - Supports a Monitor Mode
-
- Simultaneous SIP and multicast
 - Paging prioritization
 - User-uploadable ring and alert tones
 - Support for security code to prevent unwanted SIP calls
 - Can receive pages directly from Poly phones as well as other devices that can send standard multicast
 - Loud/Night Ringer function - second SIP extension
 - Support for 10 multicast paging groups
-
- Can drive an optional external analog speaker for greater coverage
 - Can support an Auxiliary Strobe for ADA-compliant visual notification
 - DTMF-controlled relay
 - Line-out connection
 - Network volume control
-
- TLS 1.2 and SRTP enhanced security for IP Endpoints in a local or cloud-based environment
 - Autoprovisioning via HTTP, HTTPS, or TFTP
 - HTTPS web based configuration
 - 802.11q VLAN tagging
 - Support for Cisco SRST/multiple SIP servers for redundancy

1.4 Supported Protocols

The SIP Speaker with Talk-Back supports:

- SIP
- Multicast
- HTTPS Web-based configuration
 - Provides an intuitive user interface for easy system configuration and verification of speaker operations.
- DHCP Client
 - Dynamically assigns IP addresses in addition to the option to use static addressing.
- HTTPS TCP Post auto-updating event notification in XML format
- SRTP
- TLS 1.2
- TFTP Client
 - Facilitates hosting for the configuration file for Autoprovisioning.
- Audio Encodings
 - PCMU (G.711 mu-law)
 - PCMA (G.711 A-law)
 - Packet Time 20 ms
 - G.722
 - G.729

1.5 Supported SIP Servers

The following link contains information on how to configure the speaker for the supported SIP servers:

<https://www.cyberdata.net/pages/connecting-to-ip-pbx-servers>

1.6 Specifications

Table 1-1. Product Specifications

Category	Specification
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
Power Input	PoE 802.3af/802.3at compliant
Audio Output	802.3af - SPL 103 dB @ 1 meter 802.3at - SPL 105 dB @ 1 meter
On-Board Relay	1A @ 30 VDC
Payload Types	G.711 a-law, G.711 μ -law, G.722, and G.729
Network Security	TLS 1.2, SRTP, HTTPS
Operating Range	Temperature: -40° C to 55° C (-40° F to 131° F) Humidity: 5-95%, non-condensing
Storage Temperature	-40° C to 70° C (-40° F to 158° F)
Storage Altitude	Up to 15,000 ft. (4573 m)
Dimensions ^a	9.055 in. [230 mm] Grill Diameter 7.25 in. [184.2 mm] Can Diameter 3.08 in. [76.11 mm] Depth
Weight	3.0 lbs [1.36 kg]
Boxed Weight	4.0 lbs. [1.81 kg]
Compliance	CE: EMC Directive – Class A EN 55032 & EN 55024, LV Safety Directive EN 62368-1; RoHS Compliant; FCC Part 15 Class; Industry Canada ICES-3 Class A; IEEE 802.3 Compliant; TAA Compliant
Warranty	2 Year Limited
Part number	011394

a. Dimensions are measured from the perspective of the product being upright with the front of the product facing you.

1.7 Optional Connections

Figure 1-3. Optional Connections

Function	Connections
Auxiliary 8-Ohm speaker connection (not to be used when the Clock is connected).	AUX SPEAKER OUT(-) AUX SPEAKER OUT(+)
Relay contacts rated at 30 VDC @ 1A.	RELAY NO RELAY COM
NOT USED	LINE IN (+) LINE IN (-)
Audio line - level output to external audio amplifier. 2v P-P into 10k Ohms.	LINE OUT (-) LINE OUT (+)
Button positive sense connection	SENSE (+)
Button negative sense connection	SENSE- COM
LED negative connection	LED COM
LED positive connection	LED (+)

12 - AUX SPKR OUT (-)
11 - AUX SPKR OUT (+)
10 - RELAY - NO
9 - RELAY - COM
8 - NOT USED
7 - NOT USED
6 - LINE - OUT (-)
5 - LINE - OUT (+)
4 - BTN SENSE - (+)
3 - BTN SENSE - COM
2 - LED COM
1 - LED (+)

CLASS II WIRING

Connections 1 through 4 are intended for use with the **011508 Remote Call Button**

1.8 Compliance

1.8.1 CE Statement



As of the date of manufacture, the Paging Series has been tested and found to comply with the specifications for CE marking and standards per EMC and Radio communications Compliance. This applies to the following products: 011145, 011146, 011233, 011280, 011295, 011314, 011368, and 011372.

EMC Directive - Class A Emissions, Immunity, and LV Safety Directive, RoHS Compliant.
Flammability rating on all components is 94V-0.

1.8.2 FCC Statement



This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CAUTION: Changes or modifications not expressly approved by the manufacturer responsible for compliance could void the user's authority to operate the equipment.

1.8.3 Industry Canada (IC) Compliance Statement

Operation is subject to the following two conditions:

- 1.This device may not cause interference, and
- 2.This device must accept any interference, including interference that may cause undesired operations of the device.

ICES-3 Class A

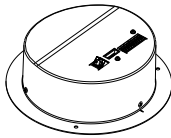
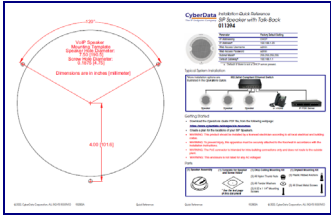
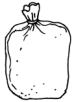
2 Installing the SIP Speaker with Talk-Back

2.1 Parts List

Table 2-1 illustrates the parts for each speaker and includes kits for the drop ceiling and drywall mounting.

Note The installation template for the SIP Speaker with Talk-Back is located on the *Installation Quick Reference Guide* that is included in the packaging with each speaker.

Table 2-1. Parts

Quantity	Part Name	Illustration
1	SIP Speaker with Talk-Back Assembly	
1	Installation Quick Reference Guide	
1	Speaker Mounting Accessory Kit (Part #070054A)	

2.2 Device Configuration

Set up and configure each speaker *before* you mount it.

CyberData delivers each speaker with the following factory default values:

Table 2-2. Factory Network Default Settings—Default of Network

Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^a	192.168.1.23
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	255.255.255.0
Default Gateway ^a	192.168.1.1

a. Default if there is not a DHCP server present.

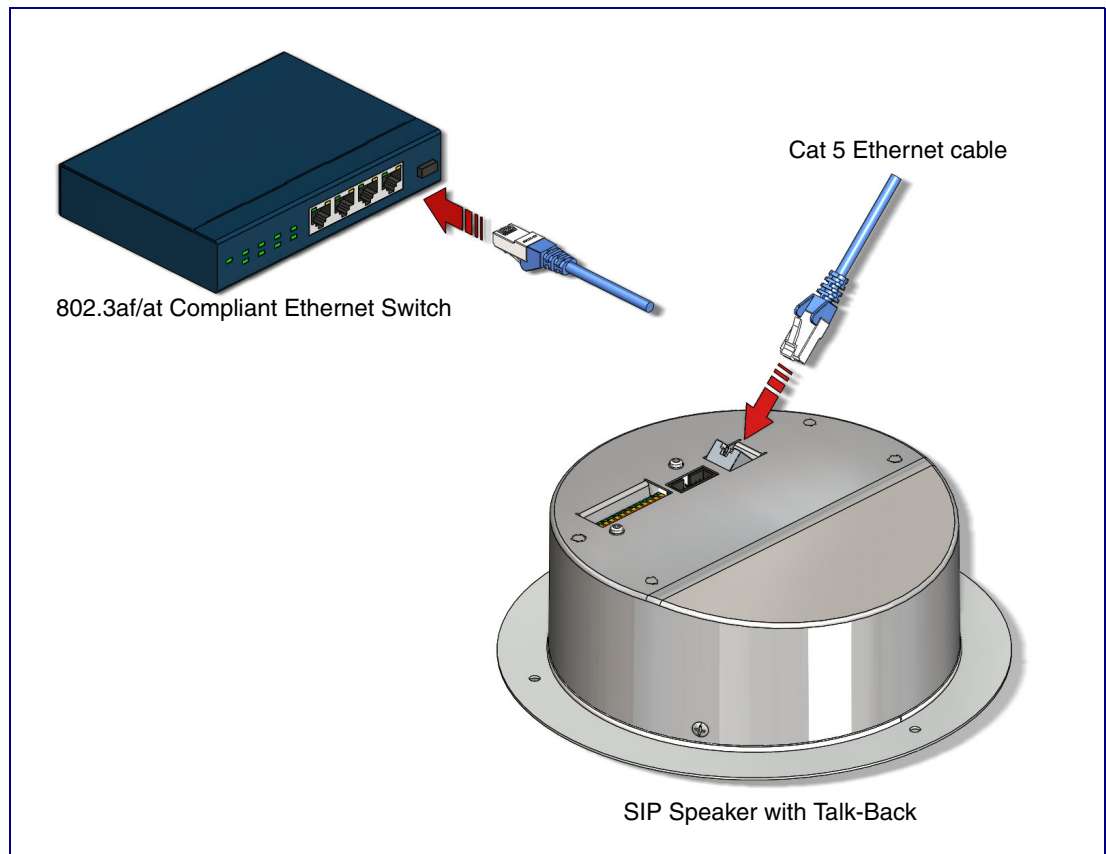
2.2.1 Connect Power to the Speaker

Figure 2-1 and Figure 2-2 illustrates how to connect power to the SIP Speaker with Talk-Back.

2.2.1.1 SIP Speaker with Talk-Back to a 802.3af Compliant PoE Switch

Figure 2-1 illustrates how to connect the SIP Speaker with Talk-Back to a 802.3af compliant PoE switch via a Cat 5 Ethernet cable.

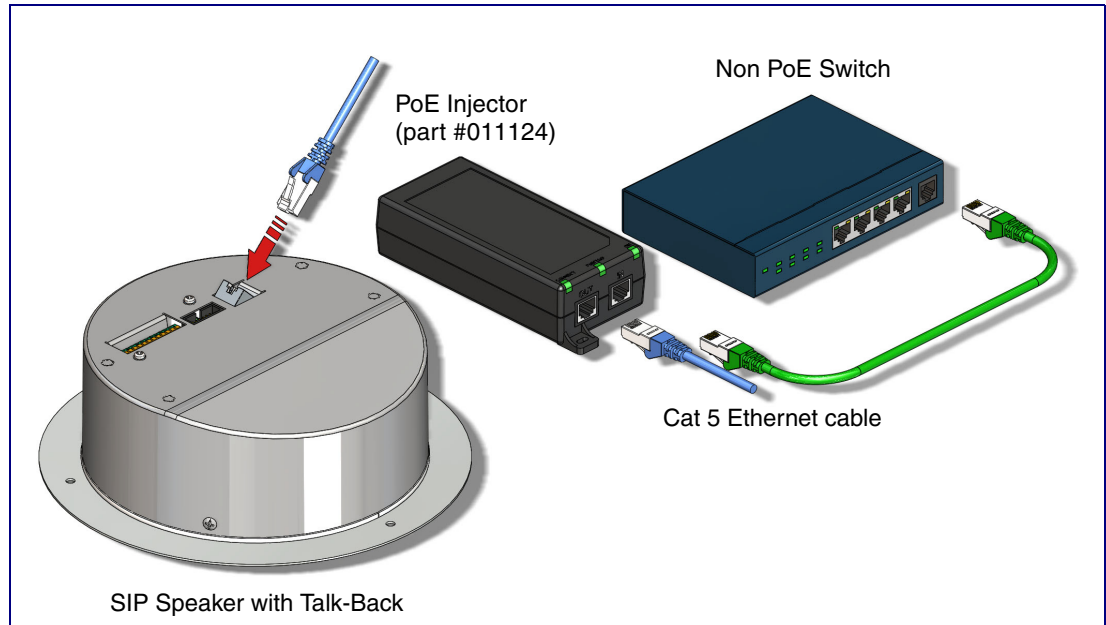
Figure 2-1. SIP Speaker with Talk-Back to a 802.3af Compliant PoE Switch



2.2.1.2 SIP Speaker with Talk-Back (with PoE Injector) to a 802.3af Compliant PoE Switch

In [Figure 2-2](#), if a PoE switch is not available, you will need a PoE Injector, part #011124 (ordered separately). A PoE Injector is a power supply solution for those who have a standard Non PoE Switch.

Figure 2-2. SIP Speaker with Talk-Back (with PoE Injector) to a Non PoE Switch



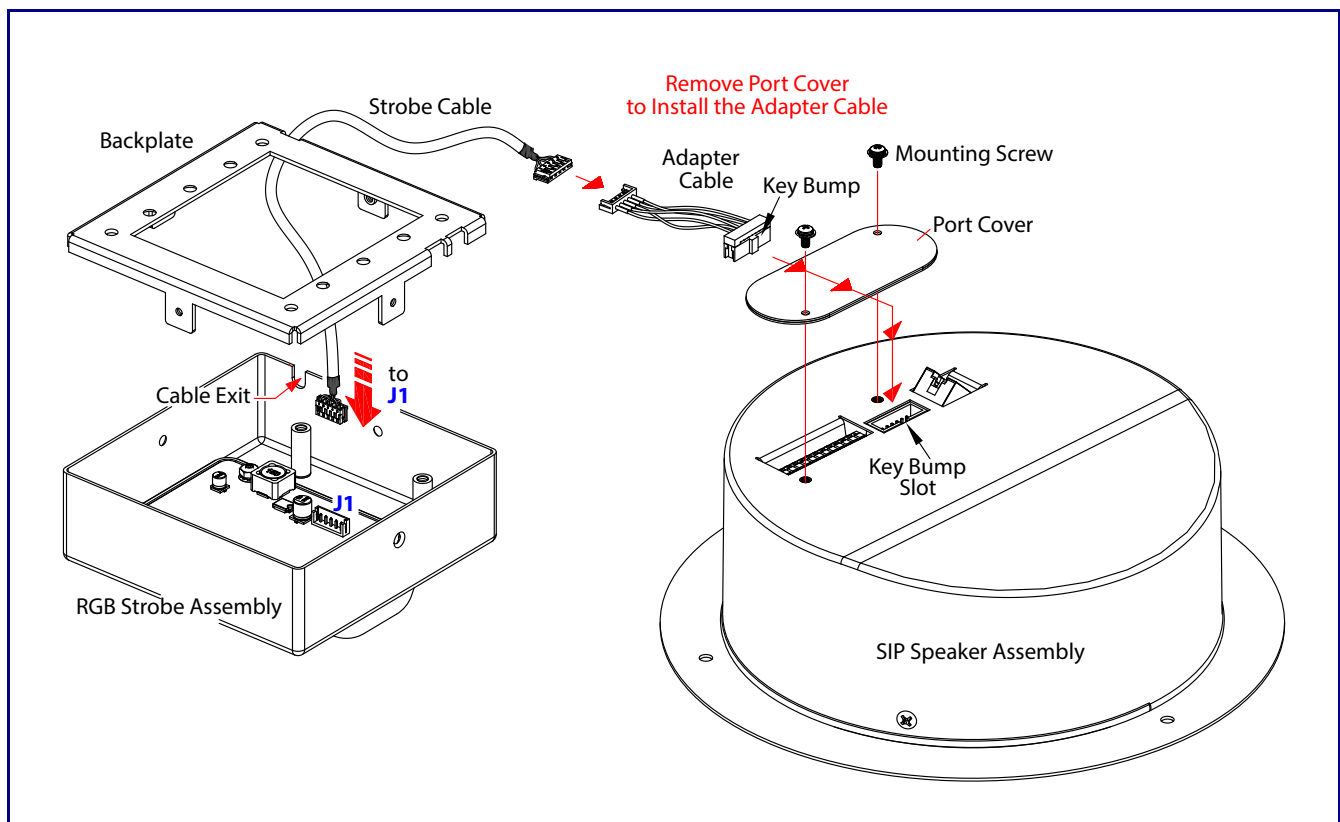
2.2.2 Installation Options

This section shows various installation options for the SIP Speaker with Talk-Back.

2.2.2.1 Connecting the Auxiliary RGB Strobe to the SIP Speaker

1. Connect the one meter strobe cable to the adapter cable. See [Figure 2-3](#).
2. Remove the mounting screws and port cover from the SIP Speaker. See [Figure 2-3](#).
3. Align the key bump on the adapter cable to the key bump slot on the SIP Speaker. See [Figure 2-3](#).
4. Replace the port cover and mounting screw. See [Figure 2-3](#).

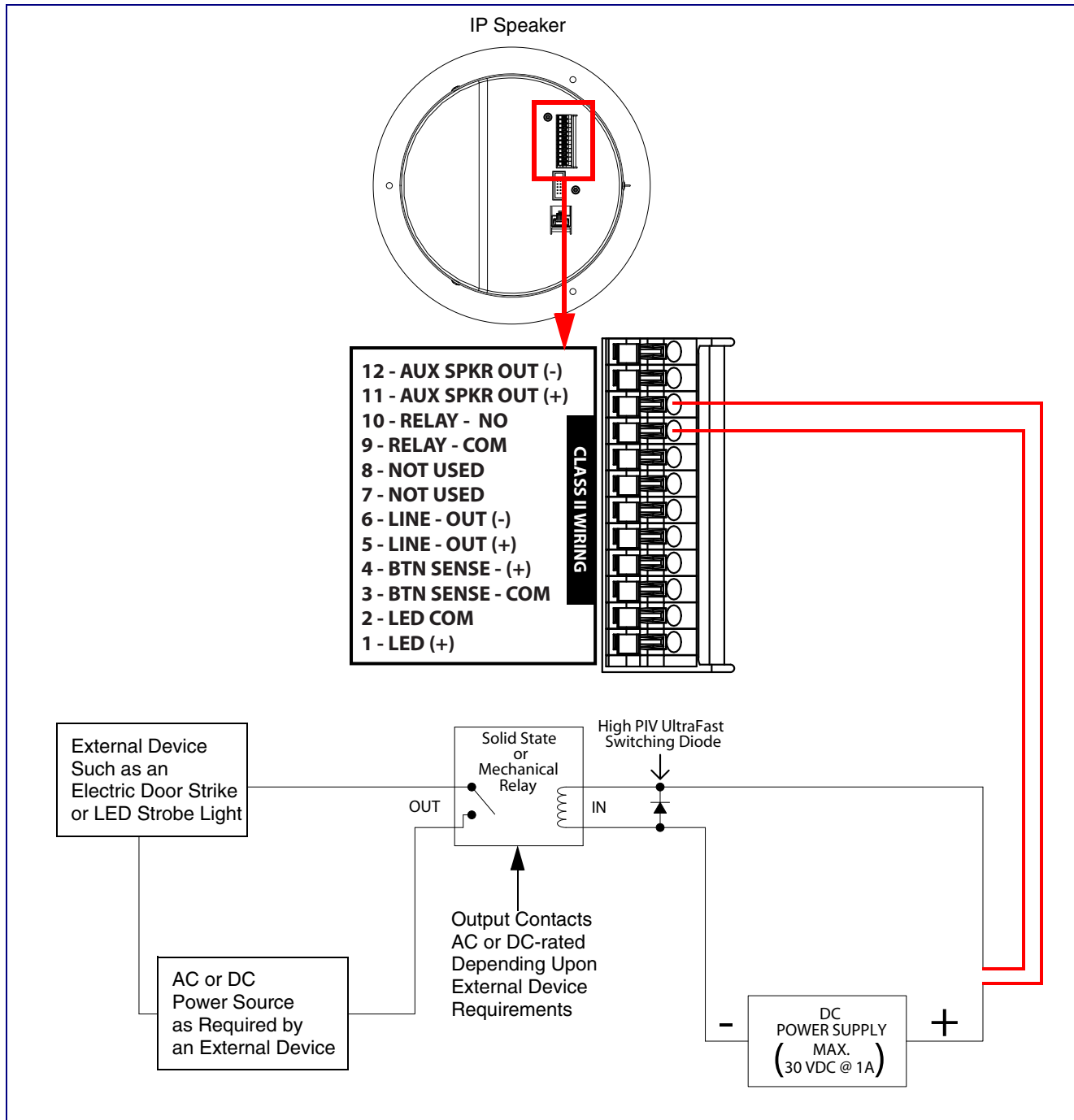
Figure 2-3. Connecting the Auxiliary RGB Strobe Kit to the SIP Speaker



2.2.2.2 SIP Speaker with Talk-Back with an External Device

In [Figure 2-4](#), when the SIP Speaker with Talk-Back is called from a remote phone, the relay on the speaker can be programmed to drive an external device such as an alert strobe. This external device may also be addressed from a separate Unified Communication (UC) server.

Figure 2-4. SIP Speaker with Talk-Back with an External Device



2.2.2.3 SIP Speaker with Talk-Back with Auxiliary Speaker Connection

In [Figure 2-5](#), the SIP Speaker with Talk-Back supports an amplified audio output for a second analog speaker. While the total speaker wattage is the same, by connecting a low cost analog speaker, additional coverage can be realized


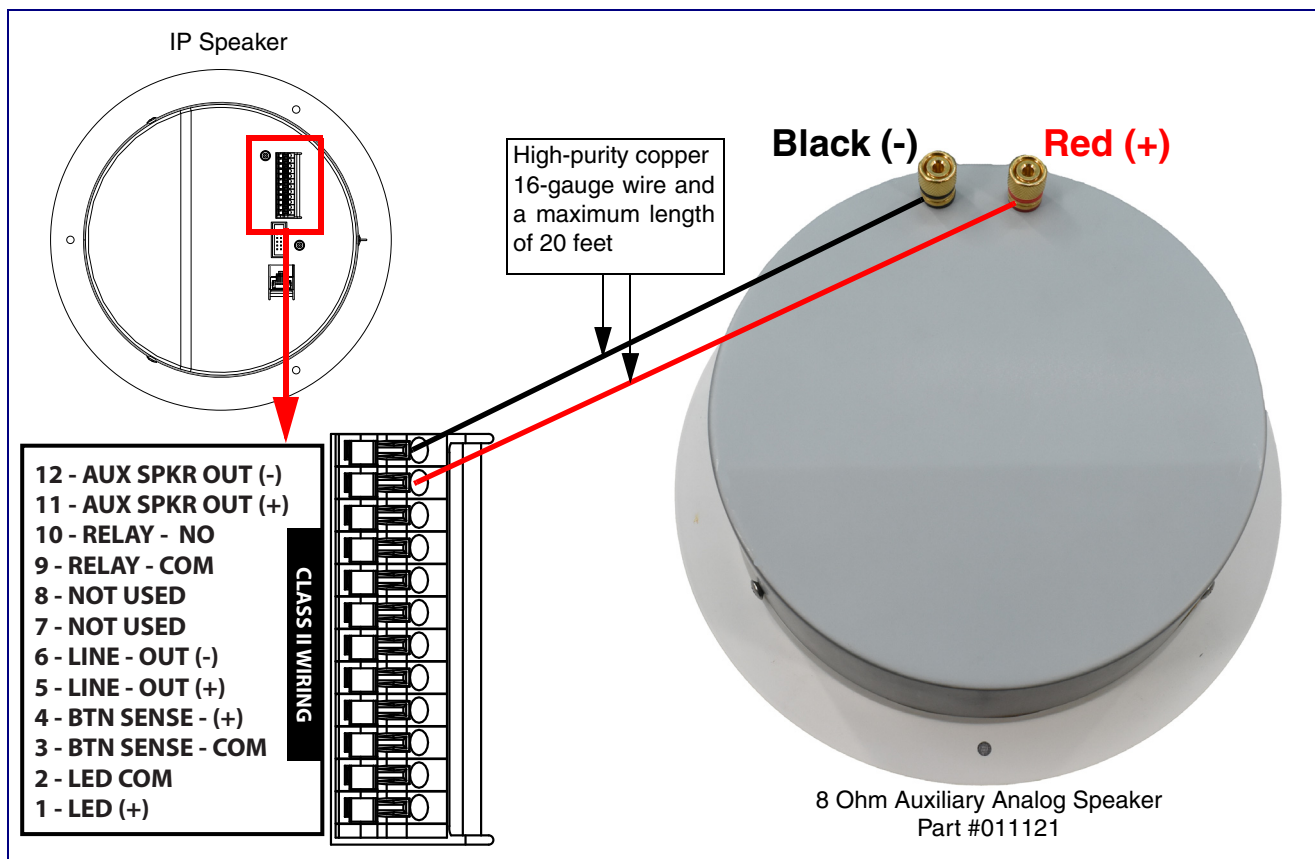
 GENERAL ALERT	Caution
<p>Operational Note: The SIP speaker dynamically adjusts volume to properly budget power when accessories are connected. For best performance, it is recommended that an 802.3AT power source is used when connecting an auxiliary speaker and a clock kit.</p>	

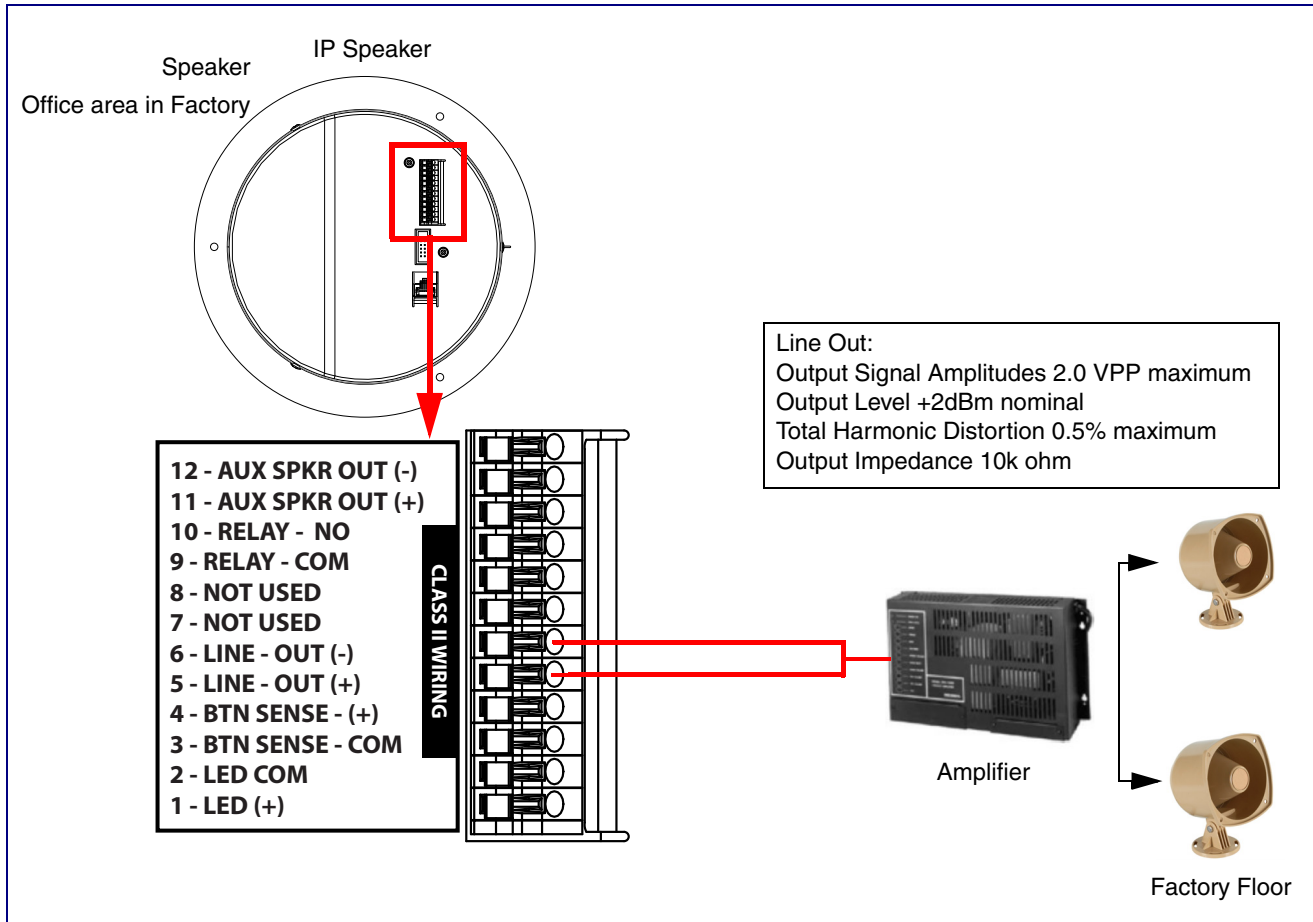
Figure 2-5. SIP Speaker with Talk-Back with Auxiliary Speaker Connection



2.2.2.4 SIP Speaker with Talk-Back with Line Out

In [Figure 2-6](#), for areas that require more speaker volume, the SIP Speaker with Talk-Back can be connected directly to an auxiliary amplifier to drive additional horns or speakers. This is done through the line-out connection.

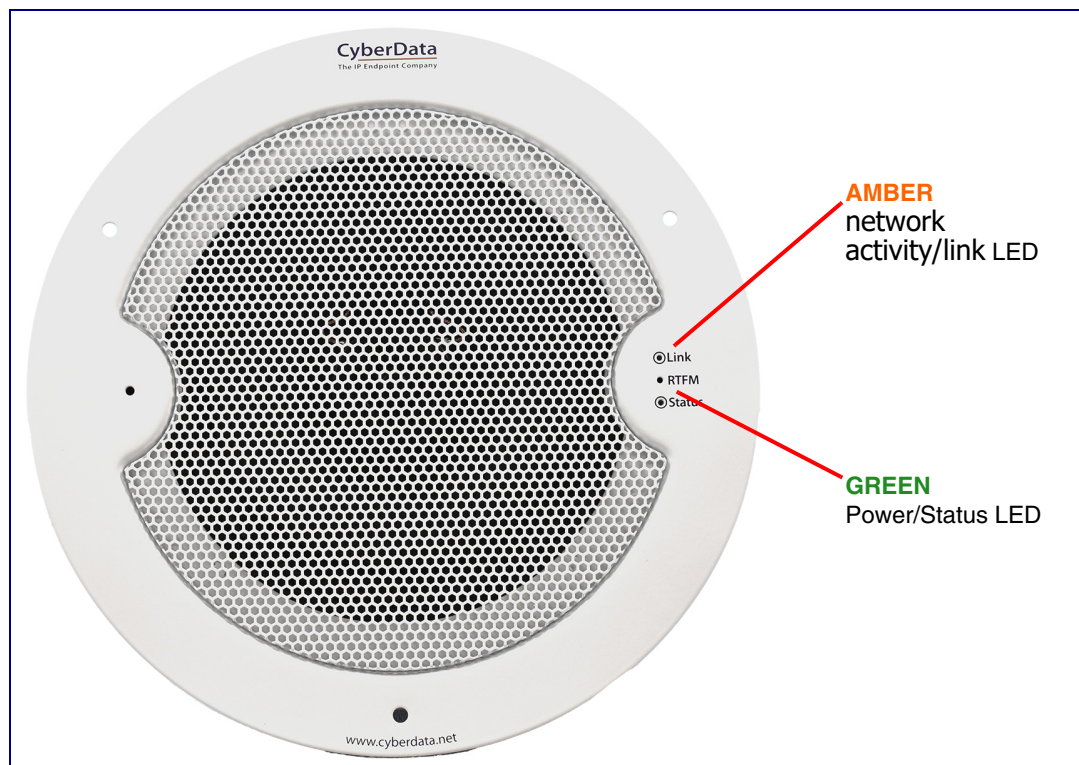
Figure 2-6. SIP Speaker with Talk-Back with Line Out



2.2.3 Confirm that the Speaker is Operational and Linked to the Network

After connecting the speaker to the 802.3af compliant Ethernet hub, the LEDs on the speaker face confirm that the speaker is operational and linked to the network.

Figure 2-7. Status and Activity LEDs



2.2.3.1 Status LED

After supplying power to the speaker:

1. The green power/status LED and the amber network activity/link LED comes on immediately.
2. After about 23 seconds with a static IP address (or 27 seconds if the board is set to use DHCP), the green LED will blink twice to indicate that the board is fully booted. The speaker will beep at this time if the **Beep on Init** option is enabled on the **Device Configuration Page** (see [Section 2.3.5, "Configure the Device"](#)).

Note If the board is set to use DHCP and there is not a DHCP server available on the network, it will try 12 times with a three second delay between tries and eventually fall back to the programmed static IP address (by default 192.168.1.23). This process will take approximately 80 seconds.

Note The front power/status LED will remain solid on during operation.

2.2.3.2 Link LED

- The **Link** LED is illuminated when the network link to the speaker is established.

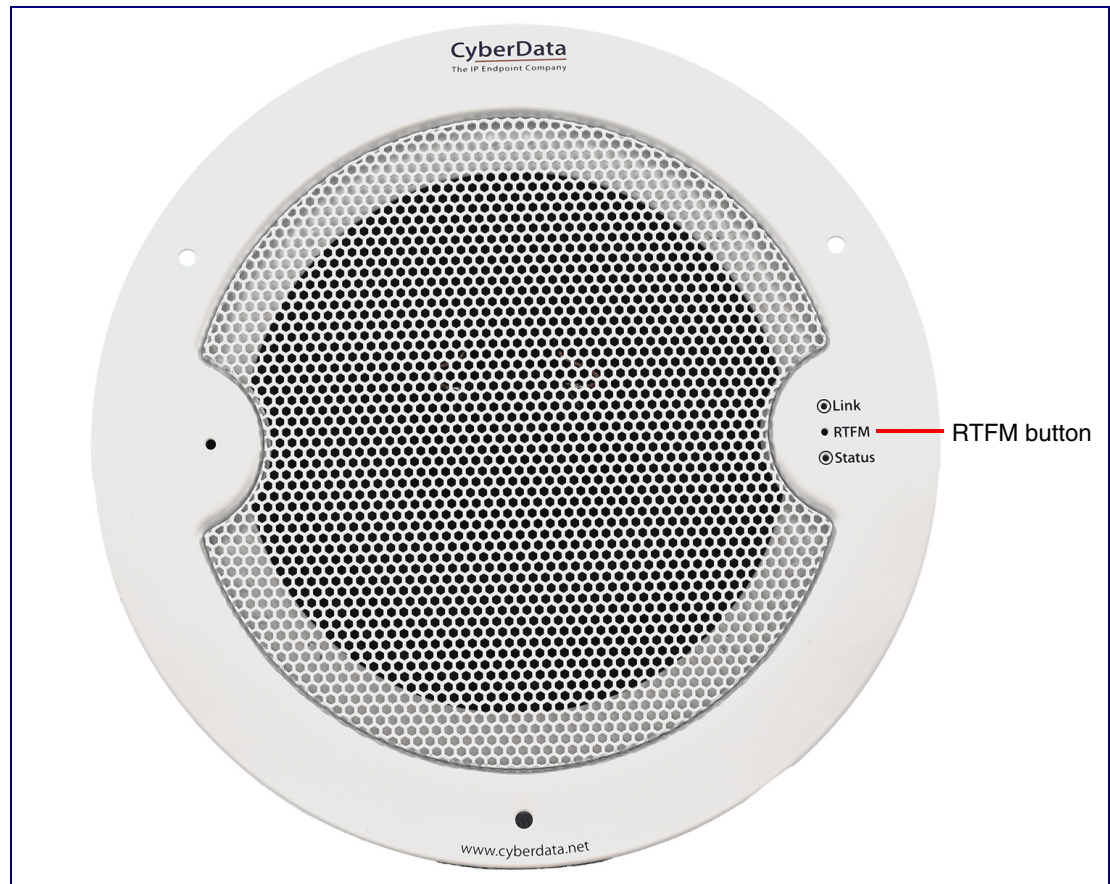
- The **Link** LED blinks to indicate network traffic.

2.2.4 Confirm the IP Address and Test the Audio

2.2.4.1 Reset Test Function Management (RTFM) Button

When the speaker is operational and linked to the network, use the Reset Test Function Management (RTFM) button (Figure 2-8) on the speaker face to announce and confirm the speaker's IP Address and test that the audio is working.

Figure 2-8. RTFM Button



To announce a speaker's current IP address, press and release the RTFM button within a five second window.

Note The speaker will use DHCP to obtain the new IP address (DHCP-assigned address or default to 192.168.1.23 if a DHCP server is not present).

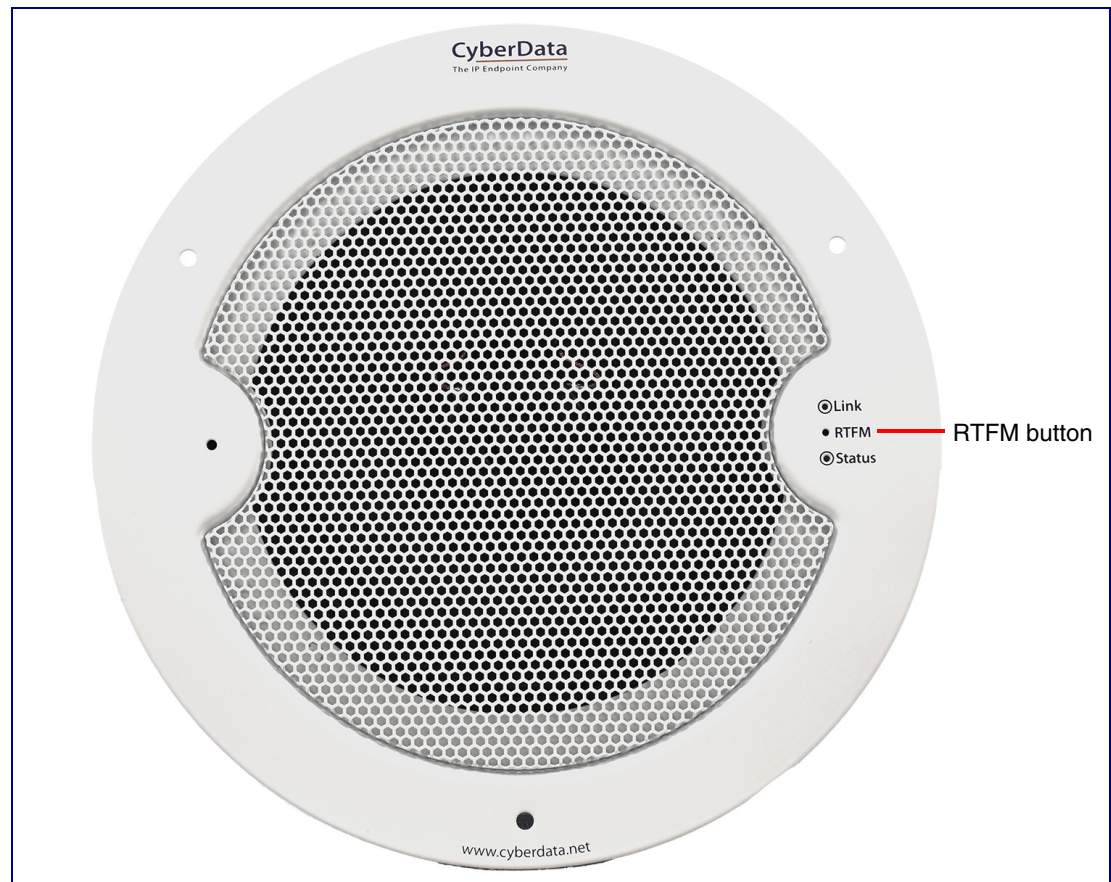
Note Pressing and holding the RTFM button for longer than five seconds will restore the speaker to the factory default settings.

2.2.5 How to Set the Factory Default Settings

2.2.5.1 RTFM Button

When the speaker is operational and linked to the network, use the Reset Test Function Management (RTFM) button (Figure 2-9) on the speaker face to set the factory default settings.

Figure 2-9. RTFM Button



To set the factory default settings:

1. Press and hold the **RTFM** button for more than five seconds.
2. The speaker announces that it is restoring the factory default settings.

Note The speaker will use DHCP to obtain the new IP address (DHCP-assigned address or default to 192.168.1.23 if a DHCP server is not present).

2.3 Configure the SIP Speaker with Talk-Back Parameters

To configure the SIP Speaker with Talk-Back online, use a standard web browser.

Configure each SIP Speaker with Talk-Back and verify its operation *before* you mount it. When you are ready to mount a SIP Speaker with Talk-Back, refer to [Appendix A, "Mounting the Speaker"](#) for instructions.

2.3.1 Factory Default Settings

All SIP Speakers with Talk-Back are initially configured with the following default IP settings:

When configuring more than one SIP Speaker with Talk-Back, attach the SIP Speakers with Talk-Back to the network and configure one at a time to avoid IP address conflicts.

Table 2-3. Factory Default Settings


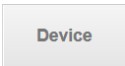
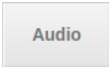
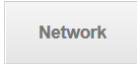

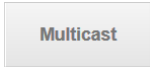

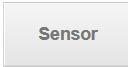
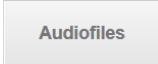
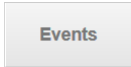


Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^a	192.168.1.23
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	255.255.255.0
Default Gateway ^a	192.168.1.1

a. Default if there is not a DHCP server present.

2.3.2 SIP Speaker with Talk-Back Web Page Navigation

Table 2-4 shows the navigation buttons that you will see on every SIP Speaker with Talk-Back web page.

Table 2-4. Web Page Navigation

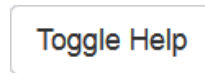
Web Page Item	Description
	Link to the Home page.
	Link to the Device page.
	Link to the Audio page.
	Link to the Network page.
	Link to go to the SIP page.
	Link to the Multicast page.
	Link to the SSL page.
	Link to the Sensor page.
	Link to the Audiofiles page.
	Link to the Events page.
	Link to the Autoprovisioning page.
	Link to the Firmware page.

2.3.3 Using the Toggle Help Button

The **Toggle Help** button allows you to see a short description of some of the settings on the webpage. To use the **Toggle Help** button, do the following:

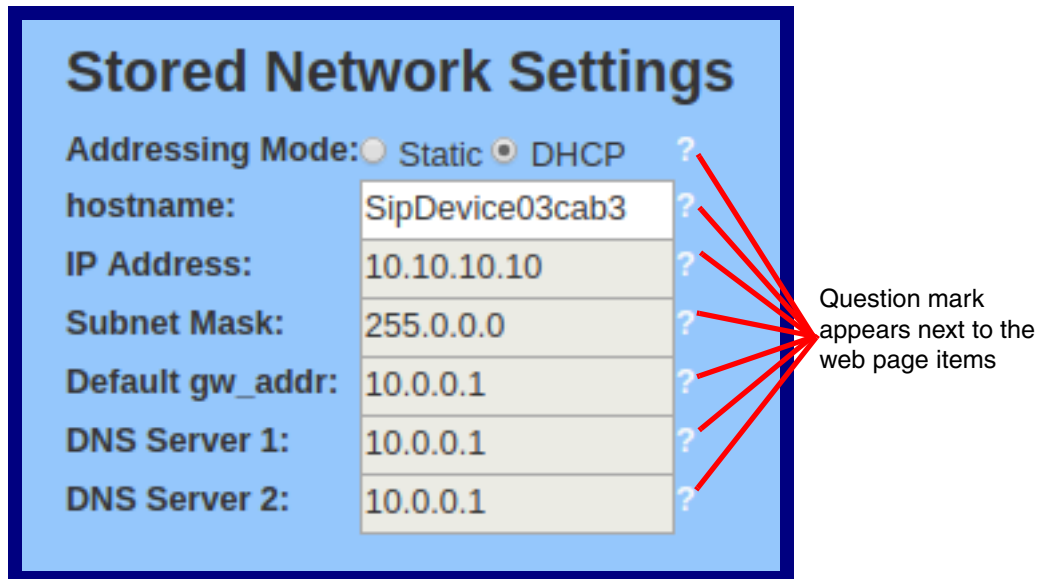
1. Click on the **Toggle Help** button that is on the UI webpage. See [Figure 2-10](#) and [Figure 2-11](#).

Figure 2-10. Toggle/Help Button



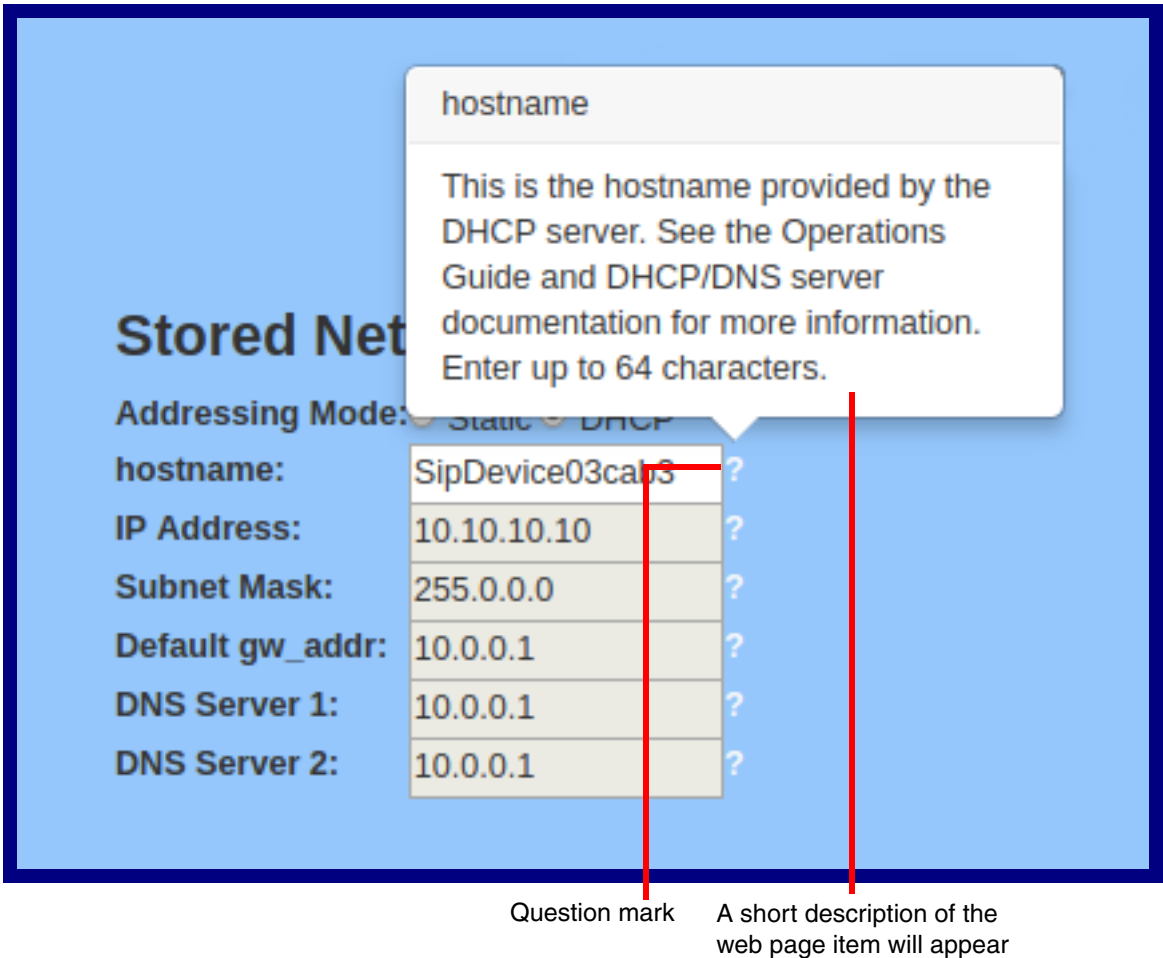
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See [Figure 2-11](#).

Figure 2-11. Toggle Help Button and Question Marks



- 3. Move the mouse pointer to hover over the question mark (?), and a short description of the web page item will appear. See Figure 2-12.

Figure 2-12. Short Description Provided by the Help Feature



2.3.4 Log in to the Configuration Home Page

1. Open your browser to the SIP Speaker with Talk-Back IP address.

Note If the network does not have access to a DHCP server, the device will default to an IP address of 192.168.1.23.

Note Make sure that the PC is on the same IP network as the SIP Speaker with Talk-Back.

Note You may also download CyberData's VoIP Discovery Utility program which allows you to easily find and configure the default web address of the CyberData VoIP products.

CyberData's VoIP Discovery Utility program is available at the following website address:

<https://www.cyberdata.net/pages/discovery>

Note The device ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

2. When prompted, use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 2-13):

Web Access Username: **admin**

Web Access Password: **admin**

Figure 2-13. Home Page

HomeDeviceAudioNetworkSIPSSLMulticastSensorAudiofilesEventsAutoprovFirmware

CyberData SIP Speaker

Current Status

Serial Number:394200001
Mac Address:00:20:f7:04:e3:35
Firmware Version:v20.5.0
Partition 2:v20.5.0
Partition 3:v20.5.0
Booting From:partition 2

Boot From Other Partition

IP Addressing:DHCP
IP Address:10.10.0.17
Subnet Mask:255.0.0.0
Default Gateway:10.0.0.1
DNS Server 1:10.0.1.56
DNS Server 2:

SIP Volume:4
Multicast Volume:4
Ring Volume:4
Sensor Volume:4
Push to Talk Volume:4
Volume Boost:0

Microphone Gain:4
Push to Talk Microphone Gain:4

SIP Mode:Enabled
Multicast Mode:Disabled
Event Reporting:Disabled

Primary SIP Server:Not registered
Backup Server 1:Not registered
Backup Server 2:Not registered
Nightringer Server:Not registered
Monitor SIP Server:Not registered

Admin Settings

Username:admin
Password:*****
Confirm Password:*****

SaveRebootToggle Help

Import Settings

Browse...

No file chosen

Import Config

Export Settings

Export Config

Operations Guide

932005C

CyberData Corporation

3. On the **Home** page, review the setup details and navigation buttons described in [Table 2-5](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-5. Home Page Parameters

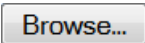




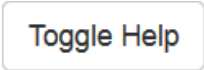
Web Page Item	Description
Admin Settings	
Username ?	The username to access the web interface. Enter up to 25 characters.
Password ?	The password to access the web interface. Enter up to 25 characters.
Confirm Password ?	Confirm the web interface password.
Current Status	
Serial Number	Shows the device serial number.
Mac Address	Shows the device Mac address.
Firmware Version	Shows the current firmware version.
IP Addressing	Shows the current IP addressing setting (DHCP or static).
IP Address	Shows the current IP address.
Subnet Mask	Shows the current subnet mask address.
Default Gateway	Shows the current default gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
SIP Mode	Shows the current status of the SIP mode.
Multicast Mode	Shows the current status of the Multicast mode.
Event Reporting	Shows the current status of the Event Reporting mode.
Nightringer	Shows the current status of the Nightringer mode.
Primary SIP Server	Shows the current status of the Primary SIP Server.
Backup Server 1	Shows the current status of Backup Server 1.
Backup Server 2	Shows the current status of Backup Server 2.
Nightringer Server	Shows the current status of Nightringer Server.
Monitor SIP Server	Shows the current status of the Monitor SIP Server.
Import Settings	
	Use this button to select a configuration file to import.
	After selecting a configuration file, click Import to import the configuration from the selected file. Then, click Save to store changes.
Export Settings	
	Click Export to export the current configuration to a file.

Table 2-5. Home Page Parameters (continued)

Web Page Item	Description
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.5 Configure the Device

1. Click the **Device** menu button to open the **Device** page. See [Figure 2-14](#).

Figure 2-14. Device Configuration Page

Home Device Audio Network SIP SSL Multicast Sensor Audiofiles Events Autoprov Firmware

CyberData SIP Speaker

Relay Settings

Activate Relay with DTMF code: ☐

Relay Pulse Code:

Relay Pulse Duration (seconds):

Relay Activation Code:

Relay Deactivation Code:

Activate Relay During Ring: ☐

Activate Relay During Night Ring: ☐

Activate Relay While Call Active: ☐

Activate Relay On Button Press: ☐

Relay On Button Press Duration:

Activate Relay While Sensor Active: ☐

DTMF Settings

Require Security Code: ☐

Security Code:

Monitor DTMF Toggle Key:

Misc Settings

Device Name:

Beep on Init: ☐

Two Speakers Connected: ☐

RGB Strobe Status: Installed

Time Settings

Enable NTP: ☒

NTP Server:

Timezone:

Current Time: Tue, 08 Nov 2022 12:29:56

Power Settings

802.3AT Mode: ☐ Not detected. Disabled

Force 802.3AT Mode (NOT recommended): ☐

Save Reboot Toggle Help Test Relay

Clock Settings

Clock Kit: Not Installed

Clock Brightness:

Use Ambient Light Sensor: ☐

Clock Colon Type: ☒ Off ☐ On ☐ Blink

Use 24 Hour Format: ☐

2. On the **Device** page, you may enter values for the parameters indicated in [Table 2-6](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.




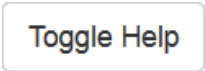
Table 2-6. Device Configuration Parameters

Web Page Item	Description
Relay Settings	
Activate Relay with DTMF Code ?	Activates the relay when the DTMF Activation Code is entered on the phone during a SIP call with the device. RFC2833 DTMF payload types are supported.
Relay Pulse Code ?	DTMF code used to pulse the relay when entered on a phone during a SIP call with the device. Relay will activate for Relay Pulse Duration seconds then deactivate. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).
Relay Pulse Duration (in seconds) ?	The length of time (in seconds) during which the relay will be activated when the DTMF Relay Activation Code is detected. Enter up to 5 digits.
Relay Activation Code ?	Activation code used to activate the relay when entered on a phone during a SIP call with the device. Relay will be active indefinitely, or until the DTMF Relay Deactivation code is entered. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).
Relay Deactivation Code ?	Code used to deactivate the relay when entered on a phone during a SIP call with the device. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).
Activate Relay During Ring ?	When selected, the relay will be activated for as long as the device is ringing. When Auto-Answer Incoming Calls is enabled, the device will not ring and this option does nothing.
Activate Relay During Night Ring ?	When selected, the relay will be activated as long as the Nightringer extension is ringing.
Activate Relay While Call Active ?	When selected, the relay will be activated as long as the SIP call is active.
Activate Relay On Button Press ?	When selected, the relay will be activated when the Call button is pressed.
Relay On Button Press Duration ?	The length of time (in seconds) during which the relay will be activated when the Call button is pressed. Enter up to 5 digits. A Relay on Button Press Duration value of 0 will pulse the relay once when the Call button is pressed.
Activate Relay While Sensor Active ?	When selected, the device's on-board relay will be activated until the on-board sensor is deactivated.
Time Settings	
Enable NTP ?	Sync device's local time with the specified NTP Server.
NTP Server ?	Use this field to set the address (in IPv4 dotted decimal notation or as a canonical name) for the NTP Server. This field can accept canonical names of up to 64 characters in length.

Table 2-6. Device Configuration Parameters (continued)

Web Page Item	Description
Timezone	Enter the tz database string of your timezone. Examples: America/Los_Angeles America/New_York Europe/London America/Toronto See https://en.wikipedia.org/wiki/List_of_tz_database_time_zones for a full list of valid strings.
Current Time	Displays the current time.
Clock Settings	These settings will only appear if you are using the Clock Kit. If you are not using the Clock Kit, you will see the words NOT INSTALLED.
Clock Kit ?	Displays the status of optional Clock Kit.
Clock Brightness (0 - 14) ?	This setting allows you to select the clock brightness level (0-14).
Use Ambient Light Sensor ?	This setting enables or disables the ambient light sensor.
Clock Colon Type ?	This setting allows you to select the clock colon type.
Use 24 Hour Time ?	When selected, the time will be show in 24 hour format on the optional clock display.
DTMF Settings	
Require Security Code ?	When selected, the user will be prompted to enter a Security Code (entered on this page) before being able to execute a page when calling the device.
Security Code ?	Type the Security Code in this field. The Security Code must only use characters '0-9', '*' and '#'. Enter up to 25 characters.
Monitor DTMF Toggle Key ?	Specify the key that toggles between monitor mode's 'talk' and 'listen' state. Defaults to '#'. Note: Some PBX's use # for other call functions
Misc Settings	
Device Name ?	Type the device name. Enter up to 25 characters.
Beep on Init ?	Device will play the user-defined "pagetone" audio file when it boots.
Two Speakers Connected ?	Select this option if two speakers (main and auxiliary) are connected to the board.
RGB Strobe Status ?	Status of optional RGB Strobe.
Power Settings	
802.3AT Mode ?	This device automatically detects if it is plugged into an 802.3AT (also known as PoE Plus) power source. 802.3AT provides more power than older 802.3AT power sources and allows this speaker to play audio at higher volumes. If you are sure this speaker is connected to an 802.3AT power source, but it is not being detected correctly, you can override the automatic settings below.
Force 802.3AT Mode (NOT recommended) ?	Enable this option if you are sure this speaker is connected to an 802.3AT power source, but it is not being detected correctly (not recommended).

Table 2-6. Device Configuration Parameters (continued)

Web Page Item	Description
	Click on the Test Relay button to do a relay test.
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.6 Configure the Audio

1. Click the **Audio** menu button to open the **Audio** page. See [Figure 2-14](#).

Figure 2-15. Audio Page

HomeDeviceAudioNetworkSIPSSLMulticastSensorAudiofilesEventsAutoprovFirmware

CyberData SIP Speaker

Volume Settings (0-9)

Enable Ambient Noise Compensation (ANC)☐

SIP Volume:

4

Multicast Volume:

4

Ring Volume:

4

Sensor Volume:

4

Push to Talk Volume:

4

Volume Boost:

No Volume Boost

Test Audio

Microphone Settings (0-9)

Microphone Gain:

4

Push to Talk Microphone Gain:

4

Test Microphone

Audio Health Check Log

File not found

Download Health Check Log

Remove Health Check Log

Audio Health Check

Schedule Audio Health Check:☐

Run once per:

Day

Week

Month

Time of Day (HH:MM):

00

:

00

Day of Week:

Sunday

Day of Month (1-31):

1

Run Audio Health Check

Talkback Mode

Enable Full-Duplex:☐

Voice-Operated Switch

Enable Voice-Operated Switch (VOX):☐

Push to Talk

Enable Push to Talk (PTT):☐

Enable DTMF Push to Talk (PTT):☐

Save

Reboot

Toggle Help

Operations Guide

932005C

CyberData Corporation

2. On the **Device** page, you may enter values for the parameters indicated in [Table 2-6](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed..

Table 2-7. Audio Page Parameters



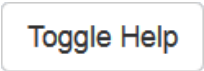
Web Page Item	Description
Volume Settings (0-9)	
Enable Ambient Noise Compensation ?	When selected, the device will measure the ambient sound level in the area and adjust the volume of the speaker accordingly.
SIP Volume ?	Set the speaker volume for a SIP call. A value of 0 will mute the speaker during SIP calls.
Multicast Volume ?	Set the speaker volume for multicast audio streams. A value of 0 will mute the speaker during multicasts.
Ring Volume ?	Set the ring volume for incoming calls. A value of 0 will mute the speaker instead of playing the ring tone when Auto-Answer Incoming Calls is disabled.
Sensor Volume ?	Set the speaker volume for playing sensor activated audio. A value of 0 will mute the speaker during sensor activated audio.
Push To Talk Volume ?	Set the speaker volume for Push to Talk operation. A value of 0 will mute the speaker in Push to Talk mode.
Volume Boost: ? No Volume Boost +4dB	Set the Boost level to increase the volume output of the speaker. Using Volume Boost may introduce audio clipping and/or distortion. Boost is only recommended for use with volumes set to level 9.
	Click on the Test Audio button to do an audio test. When the Test Audio button is pressed, you will hear a voice message for testing the device audio quality and volume.
Microphone Settings (0-9)	
Microphone Gain ?	Set the microphone gain level.
Push to Talk Microphone Gain ?	Set the microphone gain level for Push to Talk operation.
	Click on the Test Microphone button to do a microphone test. When the Test Microphone button is pressed, the following occurs: 1. The device will immediately start recording 3 seconds of audio. 2. The device will play back the recorded audio.
Audio Health Check	
Schedule Audio Health Check ?	Configure the audio health check to run automatically at a specified periodic interval. See options below. Note: make sure the 'Time Settings' on the Device page are configured properly.
Run once per Day/Week/Month ?	Specify frequency at which scheduled audio health check will run. Only one may be selected.
Time of Day (HH:MM) ?	Input the time of day the scheduled audio health check will run. Time must be input in 24 hour format (e.g. 11:45pm will be input as 23:45). This setting applies to all three options above.
Day of Week ?	Select the day of the week the scheduled audio health check will run. This setting only applies when configured to run once per week.

Table 2-7. Audio Page Parameters (continued)

Web Page Item	Description
Day of Month (1-31) ?	Input the day of the month the scheduled audio health check will run. This setting only applies when configured to run once per month. If the day input exceeds the last day of a given month, then the last day of that month will be used (e.g. inputting 31 will schedule the health check to run on the last day of every month, even if the month does not have 31 days).
Run Audio Health Check	<p>The audio health check will run once this button is clicked. Once the test has completed, the results can be viewed in the Audio Health Check Log displayed on the webpage.</p> <p>Note: For accurate log timestamps, ensure the Time Settings on the Device page are properly configured.</p>
Talkback Mode	
Enable Full-Duplex ?	Enable full-duplex for two way calls; disabled by default.
Voice-operated Switch (VOX)	
Enable Voice-Operated Switch (VOX) ?	Enable voice activation switching (VOX) mode. This will allow the device to operate with adaptive half-duplex audio. If the signal playing out of the speaker is above a specified level, the microphone will be muted. This mode can be desirable if the echo experienced in full-duplex operation cannot be adequately canceled.
Push to Talk	
Enable Push to Talk (PTT) ?	This option is for noisy environments. When enabled, the microphone will be muted normally. When the Call button is pressed and held, it will unmute the microphone and allow the operator to send audio back. Using Push to Talk prevents the operator from terminating a call by pressing the Call button. The call must be terminated by the phone user.
Enable DTMF Push to Talk (PTT) ?	This option is for noisy environments. When enabled, in an active call the remote phone can force receive only audio (setting the mic gain to max and muting the speaker) by pressing the '*' key. Pressing the '#' key will force send only audio (setting the max speaker volume and muting the mic). Pressing the '0' key will restore full duplex operation with the normal microphone and speaker volume.
Audio Health Check Log	Logs the time and results of the audio health check.
Download Health Check Log	Downloads the health check log.
Remove Health Check Log	Removes the health check log.
Save	Click the Save button to save your configuration settings.
Reboot	Click on the Reboot button to reboot the system.

Table 2-7. Audio Page Parameters (continued)

Web Page Item	Description
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.7 Configure the Network Parameters

1. Click the **Network** menu button to open the **Network** page (Figure 2-16).

Figure 2-16. Network Page

HomeDeviceAudioNetworkSIPSSLMulticastSensorAudiofilesEventsAutoprovFirmware

CyberData SIP Speaker

Stored Network Settings

Addressing Mode:

Static

☒ DHCP

Hostname:

SipDevice04fef6

IP Address:

10.10.10.10

Subnet Mask:

255.0.0.0

Default Gateway:

10.0.0.1

DNS Server 1:

10.0.0.1

DNS Server 2:

10.0.0.1

DHCP Timeout in seconds:

60

VLAN Settings

VLAN ID (0-4095):

0

VLAN Priority (0-7):

0

Save

Reboot

Toggle Help

Current Network Settings

IP Address:

10.10.1.173

Subnet Mask:

255.0.0.0

Default Gateway:

10.0.0.1

DNS Server 1:

10.0.1.56

DNS Server 2:

2. On the **Network** page, enter values for the parameters indicated in [Table 2-8](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-8. Network Page Parameters



Web Page Item	Description
Stored Network Settings	
Addressing Mode ?	Select either DHCP IP Addressing or Static Addressing by marking the appropriate radio button. DHCP Addressing mode is enabled on default and the device will attempt to resolve network addressing with the local DHCP server upon boot. If DHCP Addressing fails, the device will revert to the last known IP address or the factory default address if no prior DHCP lease was established. See Section 2.3.1, "Factory Default Settings" for factory default settings. Be sure to click Save and Reboot to store changes when configuring a Static address.
Hostname ?	This is the hostname provided by the DHCP server. See the DHCP/DNS server documentation for more information. Enter up to 64 characters.
IP Address ?	Enter the Static IPv4 network address in dotted decimal notation.
Subnet Mask ?	Enter the Subnet Mask in dotted decimal notation.
Default Gateway ?	Enter the Default Gateway IPv4 address in dotted decimal notation.
DNS Server 1 ?	Enter the primary DNS Server IPv4 address in dotted decimal notation.
DNS Server 2 ?	Enter the secondary DNS Server IPv4 address in dotted decimal notation.
DHCP Timeout in seconds ?	Specify the desired time-out duration (in seconds) that the device will wait for a response from the DHCP server before reverting back to the stored static IP address. The stored static IP address may be the last known IP address or the factory default address if no prior DHCP lease was established. Enter up to 8 characters. A value of -1 will retry forever.
Current Network Settings	
IP Address	Shows the current Static IP address.
Subnet Mask	Shows the current Subnet Mask address.
Default Gateway	Shows the current Default Gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
VLAN Settings	
VLAN ID (0-4095) ?	Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits. Note: The device supports 802.1Q VLAN tagging support. The switch port connected to the device will need to be in "trunking mode" for the VLAN tags to propagate.
VLAN Priority (0-7) ?	Specify the IEEE 802.1p VLAN priority level. Enter 1 digit. A value of 0 may cause the VLAN ID tag to be ignored.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.

Table 2-8. Network Page Parameters (continued)

Web Page Item	Description
<div><div>Toggle Help</div></div>	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.8 Configure the SIP (Session Initiation Protocol) Parameters

1. Click on the **SIP** menu button to open the **SIP** page (Figure 2-17).

Figure 2-17. SIP Page—Top

The screenshot displays the 'SIP' configuration page for the CyberData SIP Speaker. The page has a blue header with the title 'CyberData SIP Speaker' and a navigation bar with tabs: Home, Device, Audio, Network, SIP (selected), SSL, Multicast, Sensor, Audiofiles, Events, Autoprovisioning, and Firmware. The main content area is divided into several sections:

- SIP Settings:** Includes checkboxes for 'Enable SIP operation' (checked), 'Register with a SIP Server' (checked), 'Buffer SIP Calls' (unchecked), 'Play Stored Message' (unchecked), 'Auto-Answer Incoming Calls' (checked), and 'Beep Before Page' (unchecked). Below these are input fields for 'Primary SIP Server' (10.0.0.253), 'Primary SIP User ID' (199), 'Primary SIP Auth ID' (199), 'Primary SIP Auth Password' (masked with asterisks), and 'Re-registration Interval (in seconds)' (360). There are also sections for 'Backup SIP Server 1' and 'Backup SIP Server 2', each with fields for Host or IP address, User ID, Auth ID, Password, and Re-registration Interval.
- Nightringer Settings:** Includes a 'SIP Server' field (Host or IP address), 'Remote SIP Port' (5060), 'Local SIP Port' (5061), 'Outbound Proxy' (Host or IP address), 'Outbound Proxy Port' (0), 'SIP User ID' (User ID), 'SIP Auth ID' (Auth ID), 'SIP Auth Password' (Password), and 'Re-registration Interval (in seconds)' (360).
- Nightringer Strobe Settings:** Includes a 'Blink Strobe on Nightringer' checkbox (unchecked), a 'Scene' dropdown (ADA), 'Brightness' (255), and 'Color' (Color). There are also 'Red', 'Green', and 'Blue' color selection buttons, each with a '255' value and a 'Preview' button.
- Call Disconnection:** Includes a 'Terminate Call after delay' field (0).
- Audio Codec Selection:** Includes a 'Codec' dropdown (Auto Select).
- RTP Settings:** Includes 'RTP Port (even)' (10500), 'Asymmetric RTP' (unchecked), 'Jitter Buffer' (50), and 'RTP Encryption (SRTP)' (Disabled).

At the bottom of the page, there are 'Save', 'Reboot', and 'Toggle Help' buttons.

The strobe settings will only appear if an Auxiliary Strobe Kit is connected to your device. If an Auxiliary Strobe Kit is not connected to your device, you will not see the strobe settings.

Figure 2-18. SIP Page—Bottom

Backup SIP Auth Password:

Password

Re-registration Interval (in seconds):

360

Monitor SIP Server:

Host or IP address

Monitor User ID:

User ID

Monitor Auth ID:

Auth ID

Monitor Auth Password:

Password

Remote SIP Port:

5060

Local SIP Port:

5060

SIP Transport Protocol:

UDP

TLS Version:

1.2 only (recommended)

Verify Server Certificate:

Outbound Proxy:

Host or IP address

Outbound Proxy Port:

0

Use Cisco SRST:

Disable rport Discovery:

Keep Alive Period:

10000

Audio Codec Selection

Codec:

Auto Select

RTP Settings

RTP Port (even):

10500

Asymmetric RTP:

Jitter Buffer:

50

RTP Encryption (SRTP):

Disabled

Save

Reboot

Toggle Help

SIP Ring Strobe Settings

Blink Strobe on Ring:

Scene

Brightness

Color

Red

Green

Blue

ADA

255

Color

255

255

255

Preview

SIP Call Strobe Settings

Blink Strobe during Call:

Scene

Brightness

Color

Red

Green

Blue

ADA

255

Color

255

255

255

Preview

MWI Strobe Settings

Blink Strobe on MWI:

Scene

Brightness

Color

Red

Green

Blue

ADA

255

Color

255

255

255

Preview

The strobe settings will only appear if an Auxiliary Strobe Kit is connected to your device. If an Auxiliary Strobe Kit is not connected to your device, you will not see the strobe settings.

2. On the **SIP** page, enter values for the parameters indicated in [Table 2-9](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-9. SIP Page Parameters

Web Page Item	Description
SIP Settings	
Enable SIP Operation ?	When enabled, the device will transmit, receive, and process SIP messages according to the configured SIP settings below.
Register with a SIP Server ?	When enabled, the device will attempt to register to the configured SIP Server(s) on this page.
Buffer SIP Calls ?	Device will buffer audio and play it back after hang up. Length of the buffer varies with codec.
Play Stored Message ?	When selected, the caller will be prompted to select one of nine stored messages to play through the speaker. Stored messages may be customized on the Audiofiles page.
Auto-Answer Incoming Calls ?	When selected, the device will automatically answer incoming calls. When Auto-Answer Incoming Calls is disabled, the device will play a ring tone (corresponds to Ring Tone on the Audiofiles page) out of the speaker until someone presses the Call button to answer the call or the caller disconnects before the call can be answered.
Beep Before Page ?	Device will play the user defined “pagetone” audio file before playing a SIP page.
Primary SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the primary SIP server. This field can accept entries of up to 255 characters in length.
Primary SIP User ID ?	Specify the SIP User ID for the Primary SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the primary SIP server. Enter up to 64 alphanumeric characters.
Primary SIP Auth ID ?	Specify the Authenticate ID for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Primary SIP Auth Password ?	Specify the Authenticate Password for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Backup SIP Server 1 ?	Enter the backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID ?	Specify the SIP User ID for the first backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the first backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID ?	Specify the Authenticate ID for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password ?	Specify the Authenticate Password for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.

Table 2-9. SIP Page Parameters (continued)

Web Page Item	Description
Backup SIP Server 2 ?	Enter a second backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the second backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID ?	Specify the SIP User ID for the second backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the second backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID ?	Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password ?	Specify the Authenticate Password for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Monitor SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the SIP server. This field can accept entries of up to 255 characters in length.
Monitor User ID ?	Specify the SIP User ID for the SIP server. This parameter becomes the user portion of the SIP-URI for the device's Monitor Mode extension. Enter up to 64 alphanumeric characters.
Monitor Auth ID ?	Specify the Authenticate ID for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Monitor Auth Password ?	Specify the Authenticate Password for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Remote SIP Port ?	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port ?	The Local SIP Port is the port number the device will use to receive SIP messages. The default Local SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
SIP Transport Protocol ?	Choose the transport protocol for SIP signaling. This will affect all extensions, including the Nighthringer. Default is UDP.
TLS Version ?	Choose the TLS version for SIP over TLS. Modern security standards strongly recommend using TLS 1.2.
Verify Server Certificate ?	When enabled, the device will verify the authenticity of the server during the TLS handshake by its certificate and common name. The TLS handshake will be aborted if the server is deemed to be inauthentic and SIP registration will not proceed.
Outbound Proxy ?	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port ?	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.

Table 2-9. SIP Page Parameters (continued)


Web Page Item	Description
Use Cisco SRST ?	When enabled, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony). It is required for use in clustered Cisco Unified Communications Manager topologies.
Disable rport Discovery ?	Disabling rport Discovery will prevent the device from including the public WAN IP address and port number in the contact information that is sent to the remote SIP servers. This will generally only need to be enabled when using an SBC or SIP ALG in conjunction with a remote SIP server.
Keep Alive Period ?	The minimum time in milliseconds between keep-alive packets sent for nat traversal. A value of 0 will disable keep alive packets.
SIP Ring Strobe Settings	The following strobe settings will only appear if an Auxiliary Strobe Kit is connected to your device. If an Auxiliary Strobe Kit is not connected to your device, you will not see the strobe settings.
Blink Strobe on Ring ?	When selected, the Strobe will blink a scene when ringing.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when there is a SIP Ring. This is the maximum brightness for “fade” type scenes.
Red ?	The red LED value for SIP Ring.
Green ?	The green LED value for SIP Ring.
Blue ?	The blue LED value for SIP Ring.
	Use this button to preview the strobe flashing behavior for the SIP Ring Strobe Settings .
SIP Call Strobe Settings	The following strobe settings will only appear if an Auxiliary Strobe Kit is connected to your device. If an Auxiliary Strobe Kit is not connected to your device, you will not see the strobe settings.
Blink Strobe during Call ?	When selected, the Strobe will blink a scene during a call.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.

Table 2-9. SIP Page Parameters (continued)













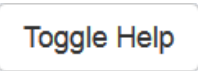

Web Page Item	Description
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when there is a SIP Call. This is the maximum brightness for "fade" type scenes.
Red ?	The red LED value for SIP Call.
Green ?	The green LED value for SIP Call.
Blue ?	The blue LED value for SIP Call.
	Use this button to preview the strobe flashing behavior for the SIP Call Strobe Settings .
MWI Strobe Settings	
The following strobe settings will only appear if you are using the Auxiliary Strobe Kit. If you are not using the Auxiliary Strobe Kit, you will not see the strobe settings.	
Blink Strobe on MWI ?	When selected, the strobe will blink a scene when a voicemail is waiting for its extension.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
MWI Call Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when there is a message waiting. This is the maximum brightness for "fade" type scenes.
Red ?	The red LED value for MWI.
Green ?	The green LED value for MWI.
Blue ?	The blue LED value for MWI.
	Use this button to preview the strobe flashing behavior for the MWI Strobe Settings .
Nightringer Settings	
SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's Nightringer extension on the SIP server. This field can accept entries of up to 255 characters in length.

Table 2-9. SIP Page Parameters (continued)

Web Page Item	Description
Remote SIP Port ?	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages for the Nightringer extension. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port ?	The Local SIP Port is the port number the device will use to receive SIP messages for the Nightringer extension. This value cannot be the same as the Local SIP Port for the primary extension. The default Local SIP Port is 5061. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy ?	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address for the Nightringer extension. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages for the Nightringer extension. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port ?	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy for the Nightringer extension. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
SIP User ID ?	Specify the SIP User ID for the SIP server. This parameter becomes the user portion of the SIP-URI for the device's Nightringer extension. Enter up to 64 alphanumeric characters.
SIP Auth ID ?	Specify the Authenticate ID for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
SIP Auth Password ?	Specify the Authenticate Password for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration Interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Nightringer Strobe Settings	The following strobe settings will only appear if you are using the Auxiliary Strobe Kit. If you are not using the Auxiliary Strobe Kit, you will not see the strobe settings.
Blink Strobe on Nightring ?	When selected, the Strobe will blink a scene when the Nightringer is ringing.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when the Nightringer is ringing. This is the maximum brightness for "fade" type scenes.
Red ?	The red LED value for Nightringer.
Green ?	The green LED value for Nightringer.

Table 2-9. SIP Page Parameters (continued)

Web Page Item	Description
Blue 	The blue LED value for Nightringer.
	Use this button to preview the strobe flashing behavior for the Nightringer Strobe Settings .
Call Disconnection	
Terminate Call After Delay 	Automatically terminate an active call after a given delay in seconds. A value of 0 will disable this function. Enter up to 8 digits.
Audio Codec Selection	
Codec 	Select desired codec (only one may be chosen).
RTP Settings	
RTP Port (even) 	Specify the port number used for the RTP stream after establishing a SIP call. This port number must be an even number and defaults to 10500. The supported range is 0-65536. Enter up to 5 digits.
Asymmetric RTP 	<p>Specify if the remote endpoint will send and receive RTP packets on different ports. If set to false, the device will track the address/port that is sending RTP packets during a SIP call. If the address/port changes mid-stream, the device will disregard the SDP and send all further RTP packets to this new address.</p> <p>If set to true, this device will ignore the sending address/port and send RTP as specified in the SDP. Warning! Enabling asymmetric RTP can cause the RTP stream to be lost.</p> <p>Most installations should not enable asymmetric RTP.</p>
Jitter Buffer 	Specify the size of the jitter buffer (in milliseconds) used for SIP calls. Valid values are 50-1000.
RTP Encryption (SRTP) 	When enabled, a SIP call's audio streams are encrypted using SRTP.
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark () appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

Note For specific server configurations, go to the following website address:

<https://www.cyberdata.net/pages/connecting-to-ip-pbx-servers>

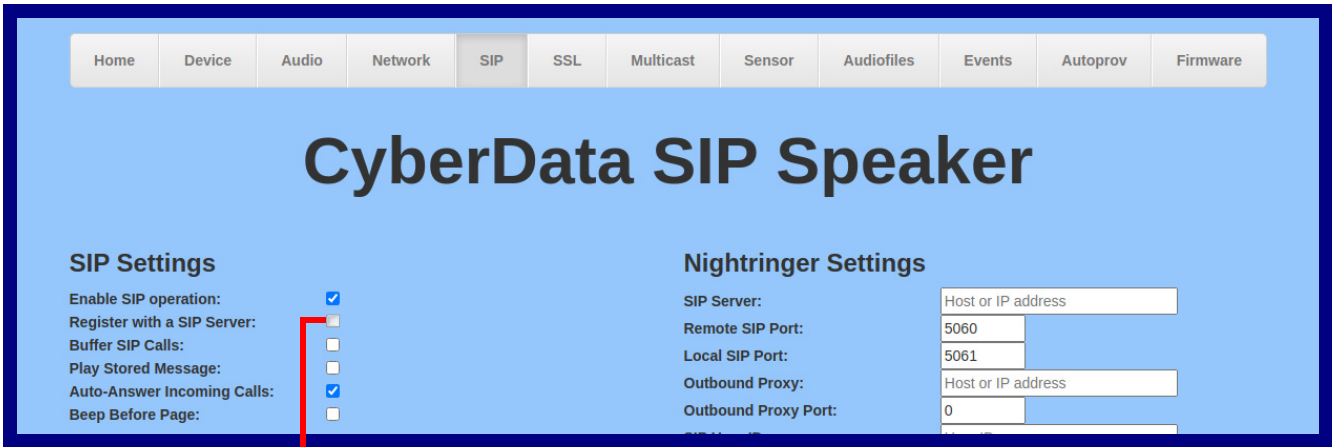
Note The maximum number of total characters in the dial-out field is 64.

2.3.8.1 Point-to-Point Configuration

When the device is set to not register with a SIP server (see [Figure 2-19](#)), it is possible for the speaker to receive Point-to-Point calls by setting the dial out extension to the IP address of the remote device. The delayed DTMF functionality is available in Point-to-Point Mode.

Note Receiving point-to-point SiP calls may not work with all phones.

Figure 2-19. SIP Page Set to Point-to-Point Mode



Device is set to NOT register with a SiP server

2.3.8.2 Delayed DTMF

On the **SIP Configuration** page the dial out extension supports the addition of comma delimited pauses and sending additional DTMF tones (using rfc2833). The first comma will pause three seconds after a call is first established with a remote device. Subsequent commas will pause for 2 seconds. A pause of one second will be sent after each numerical digit.

Table 2-10. Examples of Dial-Out Extension Strings

Extension String	Resulting Action
302	Dial out extension 302 and establish a call
302,2	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2'
302,25,,,4,,1	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2', send out DTMF tone 5, wait 6 seconds, send out DTMF tone 4, wait 4 seconds, send out DTMF tone 1

Note The maximum number of total characters in the dial-out field is 25.

2.3.9 Configure the SSL Parameters

1. Click **SSL** menu button to open the **SSL** page (Figure 2-20 and Figure 2-21).

Figure 2-20. SSL Configuration Page

HomeDeviceAudioNetworkSIPSSLMulticastSensorAudiofilesEventsAutoprovFirmware

CyberData SIP Speaker

Web Server Certificate

subject=
countryName = US
stateOrProvinceName = California
localityName = Monterey
organizationName = Cyberdata
commonName = 0020f704fef6
notBefore=Nov 2 21:14:08 2022 GMT
notAfter=Oct 30 21:14:08 2032 GMT

Browse... No file chosen

Import Web Certificate

Restore Web Certificate

SIP Client Certificate

subject=
countryName = US
stateOrProvinceName = California
localityName = Monterey
organizationName = Cyberdata
commonName = 0020f704fef6
notBefore=Nov 2 21:14:08 2022 GMT
notAfter=Oct 30 21:14:08 2032 GMT

Browse... No file chosen

Import SIP Certificate

Restore SIP Certificate

Password (optional):

Autoprovisioning Client Certificate

subject=
countryName = US
stateOrProvinceName = California
localityName = Monterey
organizationName = Cyberdata
commonName = 0020f704fef6
notBefore=Nov 2 21:14:08 2022 GMT
notAfter=Oct 30 21:14:08 2032 GMT

Browse... No file chosen

Import Autoprovisioning Certificate

Restore Autoprovisioning Certificate

Password (optional):

Download Cyberdata CA

SaveRebootToggle Help

Test TLS Connection

Server:10.0.0.253Port:5060

Test SIP ConnectionTest Autoprov Connection

List of Trusted CAs

Upload CA Certificate:Browse... No file chosen

Import CA CertificateRemove AllRestore Defaults

1CyberData_CA.pemInfoRemove

2DigiCert_Assured_ID_Root_CA.crtInfoRemove

3DigiCert_Assured_ID_Root_G2.crtInfoRemove

4DigiCert_Assured_ID_Root_G3.crtInfoRemove

5DigiCert_Global_Root_CA.crtInfoRemove

6DigiCert_Global_Root_G2.crtInfoRemove

7DigiCert_Global_Root_G3.crtInfoRemove

8DigiCert_High_Assurance_EV_Root_CA.crtInfoRemove

Figure 2-21. SSL Configuration Page

4	DigiCert_Assured_ID_Root_G3.crt	Info	Remove
5	DigiCert_Global_Root_CA.crt	Info	Remove
6	DigiCert_Global_Root_G2.crt	Info	Remove
7	DigiCert_Global_Root_G3.crt	Info	Remove
8	DigiCert_High_Assurance_EV_Root_CA.crt	Info	Remove
9	DigiCert_Trusted_Root_G4.crt	Info	Remove
10	GeoTrust_Global_CA.crt	Info	Remove
11	GeoTrust_Primary_Certification_Authority.crt	Info	Remove
12	GeoTrust_Primary_Certification_Authority_-_G2.crt	Info	Remove
13	GeoTrust_Primary_Certification_Authority_-_G3.crt	Info	Remove
14	GeoTrust_Universal_CA.crt	Info	Remove
15	GeoTrust_Universal_CA_2.crt	Info	Remove
16	Go_Daddy_Class_2_CA.pem	Info	Remove
17	Go_Daddy_Root_Certificate_Authority_-_G2.pem	Info	Remove
18	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt	Info	Remove
19	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt	Info	Remove
20	VeriSign_Universal_Root_Certification_Authority.crt	Info	Remove
21	Verisign_Class_1_Public_Primary_Certification_Authority.crt	Info	Remove
22	Verisign_Class_1_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
23	Verisign_Class_2_Public_Primary_Certification_Authority_-_G2.crt	Info	Remove
24	Verisign_Class_2_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
25	Verisign_Class_3_Public_Primary_Certification_Authority.crt	Info	Remove
26	Verisign_Class_3_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
27	thawte_Primary_Root_CA.crt	Info	Remove
28	thawte_Primary_Root_CA_-_G2.crt	Info	Remove
29	thawte_Primary_Root_CA_-_G3.crt	Info	Remove

2. On the **SSL** page, enter values for the parameters indicated in [Table 2-11](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-11. SSL Configuration Parameters

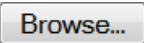


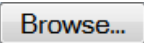


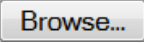
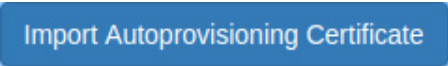
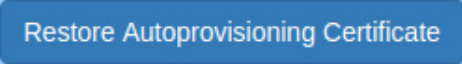


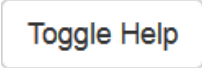

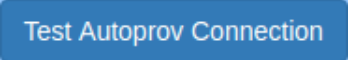
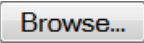




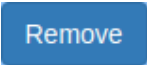
Web Page Item	Description
Web Server Certificate	Certificate used by the web server.
	Click Browse to select a certificate to import.
	After selecting a certificate, click Import Web Certificate to import it as the certificate used by this device's web server.
	Restore the device's default web server certificate. This will remove the user-uploaded Web Server Certificate. (Server CAs and Trusted CAs are unaffected).
SIP Client Certificate	When doing mutual authentication this device will present a client certificate with these parameters.
	Click Browse to select a certificate to import.
	After selecting a certificate, click Import SIP Certificate to import it as the certificate used by the device during SIP transactions.
	Restore the device's default sip client certificate. This will remove any user-uploaded sip client certificates (Server CAs and Trusted CAs are unaffected).
Password (optional) ?	Enter the optional password for the SIP certificate's private key. Note: When using a password, it must be entered and saved before importing the certificate.
Autoprovisioning Client Certificate	When doing mutual authentication this device will present a client certificate with these parameters.
	Click Browse to select a certificate to import.
	After selecting a certificate, click Import Autoprovisioning Certificate to import it as this device's certificate. This certificate will be used when requesting files during autoprovisioning.
	Restore the device's default autoprovisioning certificate. This will remove any user-uploaded autoprovisioning certificates. (Server CAs and Trusted CAs are unaffected).
Password (optional) ?	Enter the optional password for the Autoprovisioning certificate's private key. Note: When using a password, it must be entered and saved before importing the certificate.
Download Cyberdata CA ?	Right click and Save Link As... to get the Cyberdata CA used to sign this client certificate.
	Click the Save button to save your configuration settings.

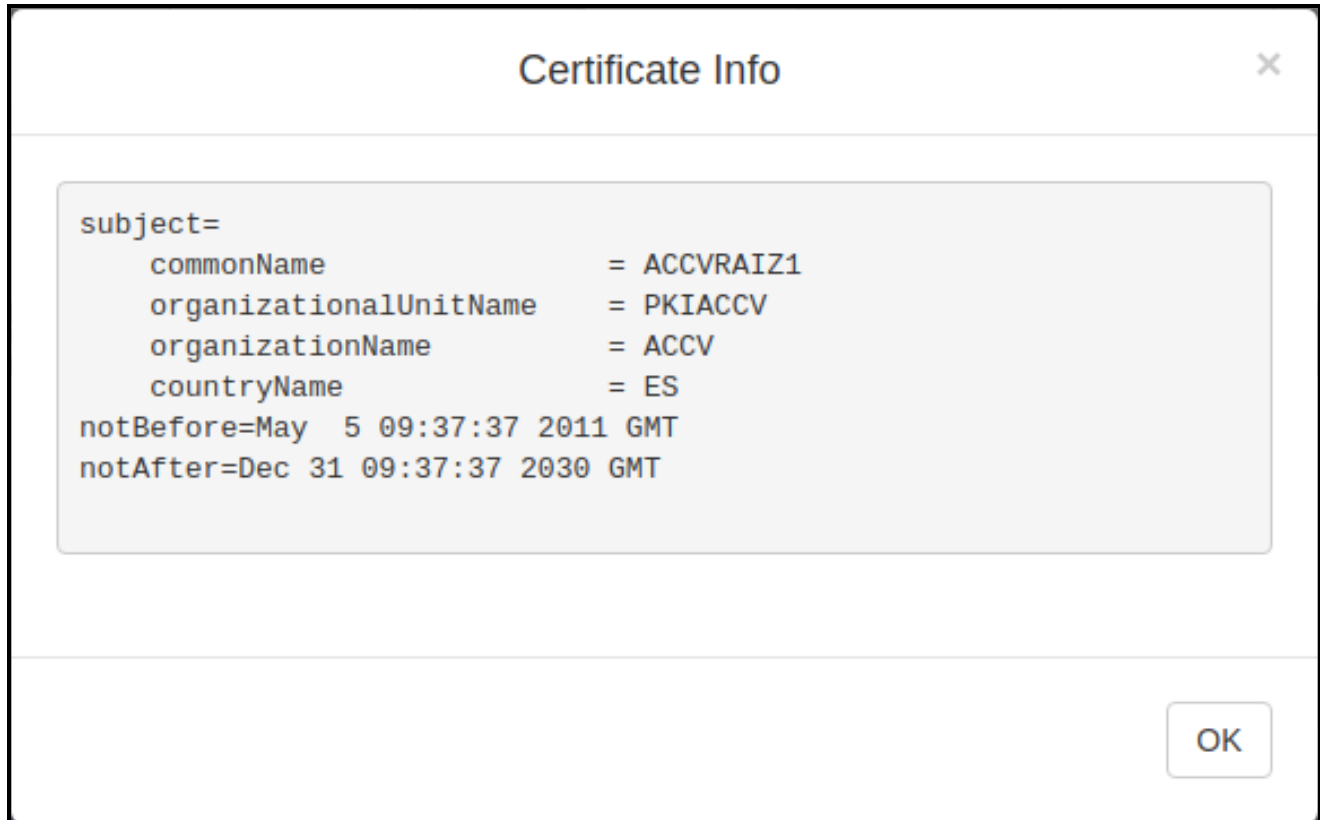
Table 2-11. SSL Configuration Parameters (continued)

Web Page Item	Description
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
Test TLS Connection	
Server ?	The ssl test server address as a fully qualified domain name or in IPv4 dotted decimal notation.
Port ?	The supported range is 0-65536. SIP connections over TLS to port 5060 are modified to connect to port 5061. This test button will do the same.
	Use this button to test a TLS connection to a remote server using the sip client key and password. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues separate from SIP registration issues.
	Use this button to test a TLS connection to a remote server using the autoprovisioning client key and password. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues with secure autoprovisioning.
List of Trusted CAs	
	Use this button to select a configuration file to import.
Upload CA Certificate ?	
	Click Browse to select a CA certificate to import. After selecting a server certificate authority (CA), click Import CA Certificate to import it to the list of trusted CAs. CAs are used to validate the certificate presented by the server when establishing a TLS connection.
	Restore Defaults will restore the default list of registered CAs and Remove All will remove all registered CAs.
	Restore Defaults will restore the default list of registered CAs and Remove All will remove all registered CAs.
	Provides details of the certificate. After clicking on this button, the Certificate Info Window appears. See Section 2.3.9.1, "Certificate Info Window" .
	Removes this certificate from the list of trusted certificates. After clicking on this button, the Remove Server Certificate Window appears. See Section 2.3.9.2, "Remove Server Certificate Window" .

2.3.9.1 Certificate Info Window

The **Certificate Info Window** provides details of the certificate. This window appears after clicking on the **Info** button. See [Figure 2-22](#).

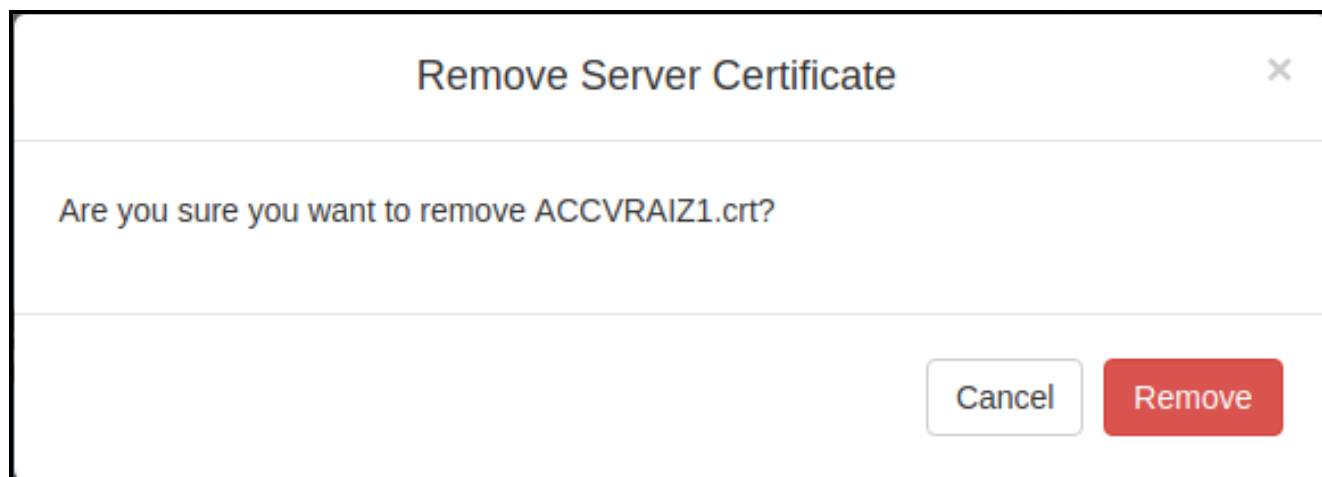
Figure 2-22. Certificate Info Window



2.3.9.2 Remove Server Certificate Window

The **Remove Server Certificate Window** will ask if the user wants to remove a certificate from the list of trusted certificates. This window appears after clicking on the **Remove** button. See [Figure 2-23](#).

Figure 2-23. Remove Server Certificate Window



2.3.10 Configure the Multicast Parameters

The Multicast Configuration page allows the device to join up to ten paging zones for receiving ulaw/alaw encoded RTP audio streams.

A paging zone can consist of one or many CyberData multicast group-enabled products. There is no limit to how many speakers can be in a given paging zone. Each multicast group is defined by a multicast address and port number.

Each multicast group is assigned a priority, allowing simultaneously arriving pages to be serviced based on importance. Multicast groups are compatible with IGMP through version 3. The device supports simultaneous SIP and Multicast.

1. Click on the **Multicast** menu button to open the **Multicast** page. See [Figure 2-24](#).

Figure 2-24. Multicast Page

Home Device Audio Network SIP SSL **Multicast** Sensor Audiofiles Events Autoprov Firmware

CyberData SIP Speaker

Multicast Settings

Enable Multicast Operation: ☒

Priority	Address	Port	Name	Buffer	Beep	Relay	Scene	Brightness	Color	Red	Green	Blue	
0	239.168.3.1	2000	Background Music	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Slow Fade ▾	50	Color ▾	70	0	128	Preview
1	239.168.3.2	3000	MG1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Fast Fade ▾	200	White		5	255	Preview
2	239.168.3.3	4000	MG2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Off ▾	255	Yellow		5	255	Preview
3	239.168.3.4	5000	MG3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	ADA ▾	255	Orange		5	255	Preview
4	239.168.3.5	6000	MG4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Fast Fade ▾	175	Red		5	255	Preview
5	239.168.3.6	7000	MG5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Slow Fade ▾	88	Pink		5	255	Preview
6	239.168.3.7	8000	MG6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	ADA ▾	255	Purple		5	255	Preview
7	239.168.3.8	9000	MG7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Slow Blink ▾	120	Blue		5	255	Preview
8	239.168.3.9	10000	MG8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Fast Blink ▾	255	Teal		5	255	Preview
9	239.168.3.10	11000	Emergency	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	ADA ▾	255	Green		5	255	Preview
									Lime			0	Preview
									Color ▾	255	255	255	Preview

Polycom Default Channel: 1 ▾
 Polycom Priority Channel: 24 ▾
 Polycom Emergency Channel: 25 ▾

SIP calls are considered priority 4.5
 Port range can be from 2000-65535
 Priority 9 is the highest and 0 is the lowest
 A higher priority audio stream will always supersede a lower one
 Priority 9 streams will play at maximum volume

Save Reboot

The strobe settings will only appear if an Auxiliary Strobe Kit is connected to your device. If an Auxiliary Strobe Kit is not connected to your device, you will not see the strobe settings.

2. On the **Multicast** page, enter values for the parameters indicated in [Table 2-12](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-12. Multicast Page Parameters





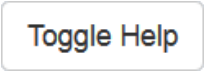
Web Page Item	Description
Enable Multicast Operation	Enables or disables multicast operation.
Priority	Indicates the priority for the multicast group. Priority 9 is the highest (emergency streams). 0 is the lowest (background music). SIP calls are considered priority 4.5 . See Section 2.3.10.1, "Assigning Priority" for more details.
Address	Enter the multicast IP Address for this multicast group (15 character limit).
Port	Enter the port number for this multicast group (5 character limit [range can be from 2000 to 65535]). Note: The multicast ports have to be even values. The webpage will enforce this restriction.
Name	Assign a descriptive name for this multicast group (25 character limit).
Buffer	Device will buffer up to four minutes of audio and then play back the recording after the multicast stream finishes or after the buffer is full.
Beep	When selected, the device will play a beep before multicast audio is sent.
Relay	When selected, the device will activate a relay before multicast audio is sent.
Scene ?	Select desired scene (only one may be chosen). Note: The strobe settings will only appear if you are using the Auxiliary Strobe Kit. If you are not using the Auxiliary Strobe Kit, you will not see the strobe settings.
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Brightness ?	How bright the strobe will blink on a multicast page. This is the maximum brightness for "fade" type scenes.
	Select desired color (only one may be chosen).
Red ?	The red LED value for Multicast.
Green ?	The green LED value for Multicast.
Blue ?	The blue LED value for Multicast.
	Use this button to preview the strobe flashing behavior for the Multicast Strobe Settings .

Table 2-12. Multicast Page Parameters (continued)

Web Page Item	Description
Polycom Default Channel	When a default Polycom channel/group number is selected, the device will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select Disabled to disable this channel.
Polycom Priority Channel	When a priority Polycom channel/group number is selected, the device will subscribe to the priority channel for one-way group pages. Group Numbers 1-25 are supported. Or, select Disabled to disable this channel.
Polycom Emergency Channel	When an emergency Polycom channel/group number is selected, the device will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select Disabled to disable this channel.
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.10.1 Assigning Priority

The device will prioritize simultaneous audio streams according to their priority in the list.

If both SIP and Multicast is enabled, SIP audio streams are considered priority **4.5**. SIP audio will interrupt multicast streams with priority **0** through **4** and will be interrupted by multicast streams with priority **5** through **9**.

During priority **9** multicast streams, the volume is set to maximum.

Note SIP calls, multicast streams, ring tones, ringback tones, and nightring tones are all prioritized.

Ringtones and Nightringtones	Ringtones all play at the same priority level. This means that it is possible to have a nightring tone and a normal ringtone playing at the same time.
------------------------------	--

2.3.11 Configure the Sensor Configuration Parameters

The door sensor (pins 5 and 6) on the header can be used to monitor a door's open or closed state. There is an option on the **Sensor** page to trigger on an open or short condition on these pins. The door sensor alarm will be activated when the **Door Open Timeout** parameter has been met.

The intrusion sensor is an optical sensor installed on the board and will be activated when the board is removed from the case.

Each sensor can trigger up to five different actions:

- Flash the LED until the sensor is deactivated (roughly 10 times/second)
- Activate the relay until the sensor is deactivated
- Loop an audio file out of the speaker until the sensor is deactivated
- Call an extension and play a pre-recorded audio file
- Call an extension and establish two way audio

Note Calling a preset extension can be set up as a point-to-point call, but currently can't send delayed DTMF tones.

1. Click **Sensor** menu button to open the **Sensor** page ([Figure 2-25](#)).

Figure 2-25. Sensor Page

HomeDeviceAudioNetworkSIPSSLMulticastSensorAudiofilesEventsAutoprovFirmware

CyberData SIP Speaker

Sensor Settings

Sensor Normally Closed: ☐ Yes ☒ No

Sensor Timeout (seconds):

Play Audio Locally: ☐

Make call to extension: ☐

Dial Out Extension:

Dial Out ID:

Play recorded audio: ☐

Repeat Sensor Message:

Button Settings

Button Installed: ☐

Button LED Lit when Idle: ☒

Button LED Brightness (0-255):

Blink button LED on monitor call: ☐

Play Ringback Tone: ☐

Prevent Call Termination: ☐

Dial Out Extension:

Dial Out ID:

Sensor Strobe Settings

Blink Strobe on Sensor: ☐

Scene	Brightness	Color	Red	Green	Blue
ADA	<input type="text" value="255"/>	<input type="text" value="Color"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>

Preview

SaveRebootToggle HelpTest SensorTest Button

The strobe settings will only appear if an Auxiliary Strobe Kit is connected to your device. If an Auxiliary Strobe Kit is not connected to your device, you will not see the strobe settings.

2. On the **Sensor** page, enter values for the parameters indicated in [Table 2-13](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-13. Sensor Page Parameters

Web Page Item	Description
Sensor Settings	
Sensor Normally Closed ?	Select the inactive state of the sensor. The sensor is also known as the Sense Input on the device's terminal block. See the Operations Guide for more information.
Sensor Timeout (in seconds) ?	The time (in seconds) the device will wait before it performs an action when the on-board door sensor is activated. The action(s) performed are based on the configured Sensor Settings below. Enter up to 5 digits.
Play Audio Locally ?	When selected, the device will loop an audio file out of the speaker until the door sensor is deactivated.
Make call to extension ?	When selected, the device will call an extension when the on-board door sensor is activated. Use the Dial Out Extension field below to specify the extension the device will call.
Dial Out Extension ?	Specify the extension the device will call when the on-board door sensor is activated. Enter up to 64 alphanumeric characters.
Dial Out ID ?	An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
Play recorded audio ?	When selected, the device will call the Dial Out Extension and play an audio file to the phone answering the SIP call (corresponds to Door Ajar on the Audiofiles page).
Repeat Sensor Message ?	The number of times to repeat the audio message through the local speaker or to the remote endpoint. A value of 0 will repeat forever. Enter a value from 0-65536.
Sensor Strobe Settings	
The following strobe settings will only appear if you are using the Auxiliary Strobe Kit. If you are not using the Auxiliary Strobe Kit, you will not see the strobe settings.	
Blink Strobe on Sensor ?	When selected, the Strobe will blink a scene when the sensor is triggered.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.

Table 2-13. Sensor Page Parameters (continued)






Web Page Item	Description
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when the sensor is triggered. This is the maximum brightness for “fade” type scenes.
Red ?	The red LED value for Sensor.
Green ?	The green LED value for Sensor.
Blue ?	The blue LED value for Sensor.
Button Settings	
Button Installed ?	When selected, the speaker is assumed to be wired to a push-to-talk button. Button settings will be enabled and sensor settings will be disabled. When not selected, the speaker is assumed to be wired to a sensor. Sensor settings will be enabled and button settings will be disabled.
Button LED Lit when Idle ?	When selected, the Call button LED is illuminated while the device is idle (a call is not in progress).
Button LED Brightness (0-255) ?	The desired Call button LED brightness level. Acceptable values are 0-255, where 0 is the dimmest and 255 is the brightest. Enter up to 3 digits.
Blink Button LED on monitor call ?	Selecting this will cause the button LED blink during a monitor call. Unselecting this will cause the speaker to give no indication that it is in a monitor call.
Play Ringback Tone ?	When selected, the device will play a ringback tone (corresponds to Ringback Tone on the Audiofiles page) out of the speaker while placing an outbound call. The Ringback Tone will play until the call is answered.
Prevent Call Termination ?	When this option is enabled, a call cannot be terminated using the call button.
Dial Out Extension ?	Specify the extension the device will call when someone presses the Call button. Enter up to 64 alphanumeric characters.
Dial Out ID ?	A Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
	Click the Test Sensor button to test the sensor.
	Click the Test Button button to test the button.
	Use this button to preview the strobe flashing behavior for the Sensor Strobe Settings .
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.

Table 2-13. Sensor Page Parameters (continued)

Web Page Item	Description
<div>Toggle Help</div>	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.12 Configure the Audiofiles Page Parameters

The **Audiofiles** page is used to add custom audio to the board. User uploaded audio will take precedence over the audio files shipped with the device.

1. Click on the **Audiofiles** menu button to open the **Audiofiles** page (Figure 2-26).

Figure 2-26. Audiofiles Page

CyberData SIP Speaker				
Available Space: 1380MB				
Audio Files				
0:	Currently set to: default	Browse...	No file chosen	Play Delete Save
1:	Currently set to: default	Browse...	No file chosen	Play Delete Save
2:	Currently set to: default	Browse...	No file chosen	Play Delete Save
3:	Currently set to: default	Browse...	No file chosen	Play Delete Save
4:	Currently set to: default	Browse...	No file chosen	Play Delete Save
5:	Currently set to: default	Browse...	No file chosen	Play Delete Save
6:	Currently set to: default	Browse...	No file chosen	Play Delete Save
7:	Currently set to: default	Browse...	No file chosen	Play Delete Save
8:	Currently set to: default	Browse...	No file chosen	Play Delete Save
9:	Currently set to: default	Browse...	No file chosen	Play Delete Save
Audio Test:	Currently set to: default	Browse...	No file chosen	Play Delete Save
Dot:	Currently set to: default	Browse...	No file chosen	Play Delete Save
Night Ring:	Currently set to: default	Browse...	No file chosen	Play Delete Save
Page Tone:	Currently set to: default	Browse...	No file chosen	Play Delete Save
Rebooting:	Currently set to: default	Browse...	No file chosen	Play Delete Save
Restoring Default:	Currently set to: default	Browse...	No file chosen	Play Delete Save
Ring Back:	Currently set to: default	Browse...	No file chosen	Play Delete Save
Ring Tone:	Currently set to: default	Browse...	No file chosen	Play Delete Save
Sensor Triggered:	Currently set to: default	Browse...	No file chosen	Play Delete Save
Stored Message File Not Found:	Currently set to: default	Browse...	No file chosen	Play Delete Save
Your IP Address Is:	Currently set to: default	Browse...	No file chosen	Play Delete Save

Figure 2-27. Audiofiles Page

Ring Tone:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Sensor Triggered:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Stored Message File Not Found:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Your IP Address Is:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>

Menu Audio Files

Cancel:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Currently Playing:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Invalid Entry:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Page:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Play Stored Message:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Pound (#):	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Through:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
To:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Enter Security Code Followed by Pound (#) key:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>

Stored Messages

Stored Message 1:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>	Repeat: <input type="text" value="0"/>	Infinite: <input type="checkbox"/>
Stored Message 2:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>	Repeat: <input type="text" value="0"/>	Infinite: <input type="checkbox"/>
Stored Message 3:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>	Repeat: <input type="text" value="0"/>	Infinite: <input type="checkbox"/>
Stored Message 4:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>	Repeat: <input type="text" value="0"/>	Infinite: <input type="checkbox"/>
Stored Message 5:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>	Repeat: <input type="text" value="0"/>	Infinite: <input type="checkbox"/>
Stored Message 6:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>	Repeat: <input type="text" value="0"/>	Infinite: <input type="checkbox"/>
Stored Message 7:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>	Repeat: <input type="text" value="0"/>	Infinite: <input type="checkbox"/>
Stored Message 8:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>	Repeat: <input type="text" value="0"/>	Infinite: <input type="checkbox"/>
Stored Message 9:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>	Repeat: <input type="text" value="0"/>	Infinite: <input type="checkbox"/>

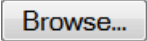

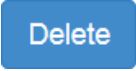

2. On the **Audiofiles** page, enter values for the parameters indicated in [Table 2-14](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-14. Audiofiles Page Parameters

Web Page Item	Description
Available Space	Shows the space available for the user to save custom audio files.
Audio Files	
0-9	<p>The name of the audio configuration option is the same as the spoken audio that plays on the board (24 character limit).</p> <p>'0' corresponds to the spoken word "zero."</p> <p>'1' corresponds to the spoken word "one."</p> <p>'2' corresponds to the spoken word "two."</p> <p>'3' corresponds to the spoken word "three."</p> <p>'4' corresponds to the spoken word "four."</p> <p>'5' corresponds to the spoken word "five."</p> <p>'6' corresponds to the spoken word "six."</p> <p>'7' corresponds to the spoken word "seven."</p> <p>'8' corresponds to the spoken word "eight."</p> <p>'9' corresponds to the spoken word "nine."</p>
Audio Test	Corresponds to the message "This is the CyberData IP speaker test message..." (24 character limit).
Dot	Corresponds to the spoken word "dot." (24 character limit).
Night Ring	Specifies the ringtone for nightring. By default this parameter uses the same audio file that is selected for the Ring Tone parameter.
Page Tone	Corresponds to a simple tone that is unused by default (24 character limit).
Rebooting	Corresponds to the spoken word "Rebooting" (24 character limit).
Restoring Default	Corresponds to the message "Restoring default" (24 character limit).
Ring Tone	Specifies the Ring Tone.
Sensor Triggered	Corresponds to the message "Sensor Triggered." (24 character limit).
Stored Message File Not Found	Corresponds to the message "Stored Message File Not Found."
Your IP Address is	Corresponds to the message "Your IP address is..." (24 character limit).
Menu Audio Files	
Menu Audio Files are user-uploadable messages that create the audio menu played to the caller.	
Cancel	Corresponds to the word "Cancel" used in the audio menu played to the caller. (24 character limit).
Currently Playing	Corresponds to the words "Currently Playing" used in the audio menu played to the caller. (24 character limit).
Invalid Entry	Corresponds to the words "Invalid Entry" used in the audio menu played to the caller. (24 character limit).
Page	Corresponds to the word "Page" used in the audio menu played to the caller. (24 character limit).

Table 2-14. Audiofiles Page Parameters (continued)

Web Page Item	Description
Play Stored Message	Corresponds to the words "Play Stored Message" used in the audio menu played to the caller. (24 character limit).
Pound (#)	Corresponds to whatever word or phrase the user wishes to call the pound key in the audio menu played to the caller (24 character limit).
Press	Corresponds to the word "Press" used in the audio menu played to the caller. (24 character limit).
Stored Message	Corresponds to the words "Stored Message" used in the audio menu played to the caller. (24 character limit).
Through	Corresponds to the word "Through" used in the audio menu played to the caller. (24 character limit).
To	Corresponds to the word "To" used in the audio menu played to the caller. (24 character limit).
Enter Security Code Followed by Pound (#) key	Corresponds to the words "Enter Security Code Followed by Pound (#) key" used in the audio menu played to the caller. (24 character limit).
Stored Messages	
Stored Message 1 through 9	<p>Stored Message 1 corresponds to the message played after pressing 1 on a phone keypad.</p> <p>Stored Message 2 corresponds to the message played after pressing 2 on a phone keypad.</p> <p>Stored Message 3 corresponds to the message played after pressing 3 on a phone keypad.</p> <p>Stored Message 4 corresponds to the message played after pressing 4 on a phone keypad.</p> <p>Stored Message 5 corresponds to the message played after pressing 5 on a phone keypad.</p> <p>Stored Message 6 corresponds to the message played after pressing 6 on a phone keypad.</p> <p>Stored Message 7 corresponds to the message played after pressing 7 on a phone keypad.</p> <p>Stored Message 8 corresponds to the message played after pressing 8 on a phone keypad.</p> <p>Stored Message 9 corresponds to the message played after pressing 9 on a phone keypad.</p>
	Click on the Browse button to navigate to and select an audio file.
	The Play button will play that audio file.
	The Delete button will delete any user uploaded audio and restore the stock audio file.
	The Save button will download a new user audio file to the board once you've selected the file by using the Browse button. The Save button will delete any pre-existing user-uploaded audio files.

2.3.12.1 User-created Audio Files

User created audio files should be saved in the following format:

RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, mono 8000 Hz

You can use the free utility *Audacity* to convert audio files into this format. See [Figure 2-28](#) through [Figure 2-30](#).

Figure 2-28. Audacity 1

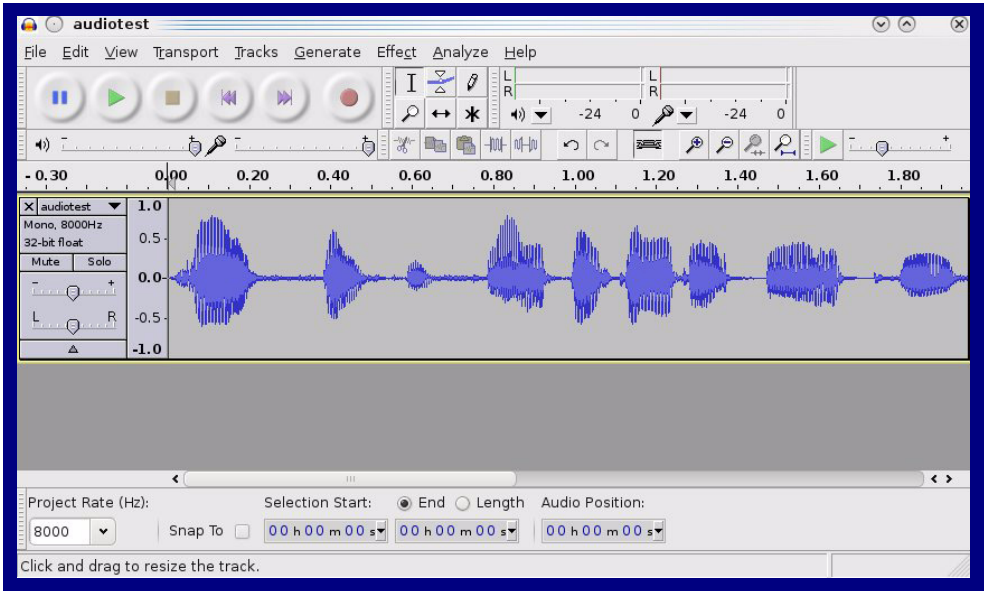
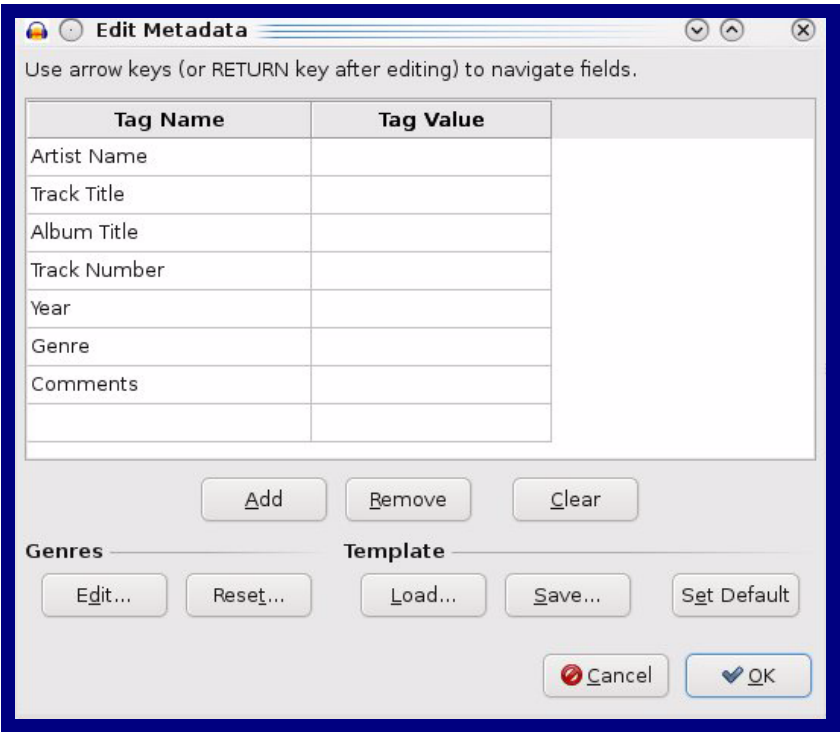


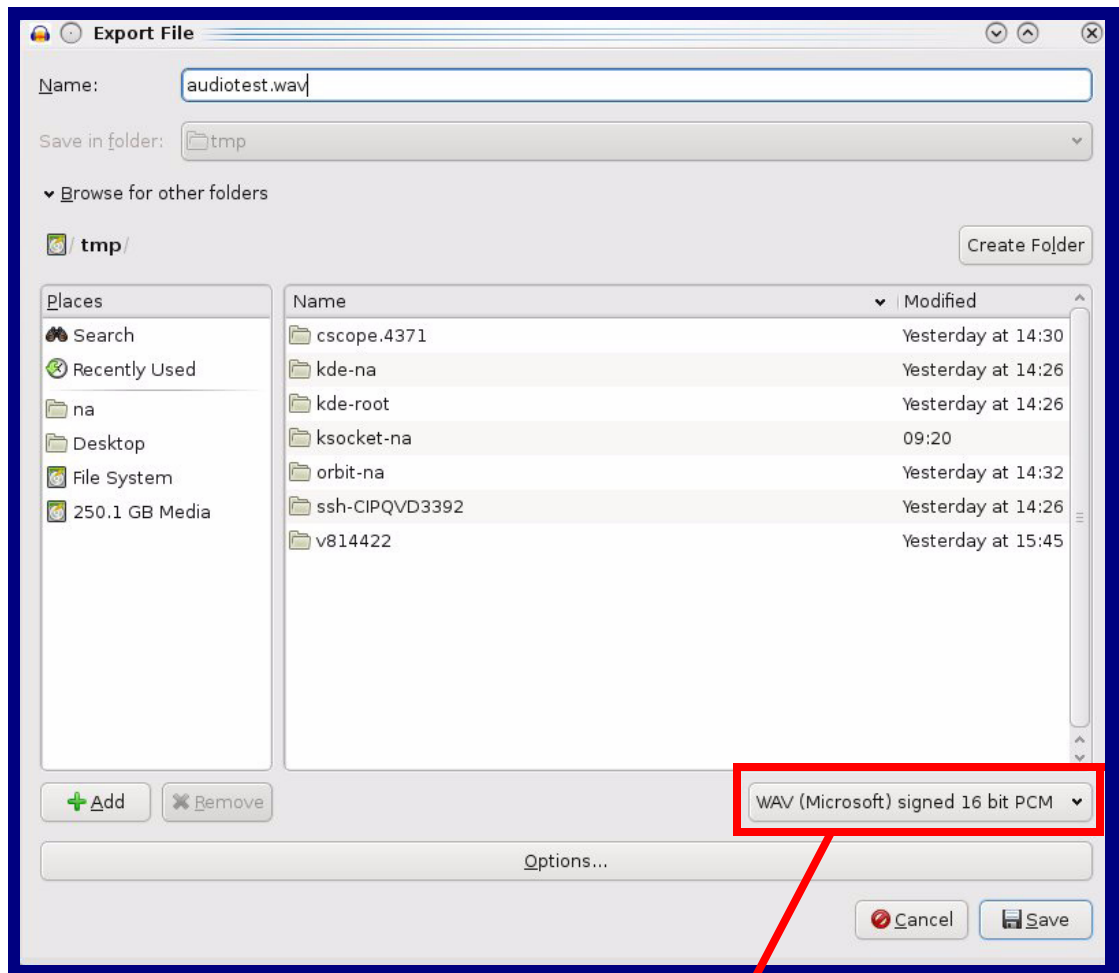
Figure 2-29. Audacity 2



When you export an audio file with Audacity, save the output as:

- **WAV (Microsoft) signed 16 bit PCM.**

Figure 2-30. WAV (Microsoft) signed 16 bit PCM



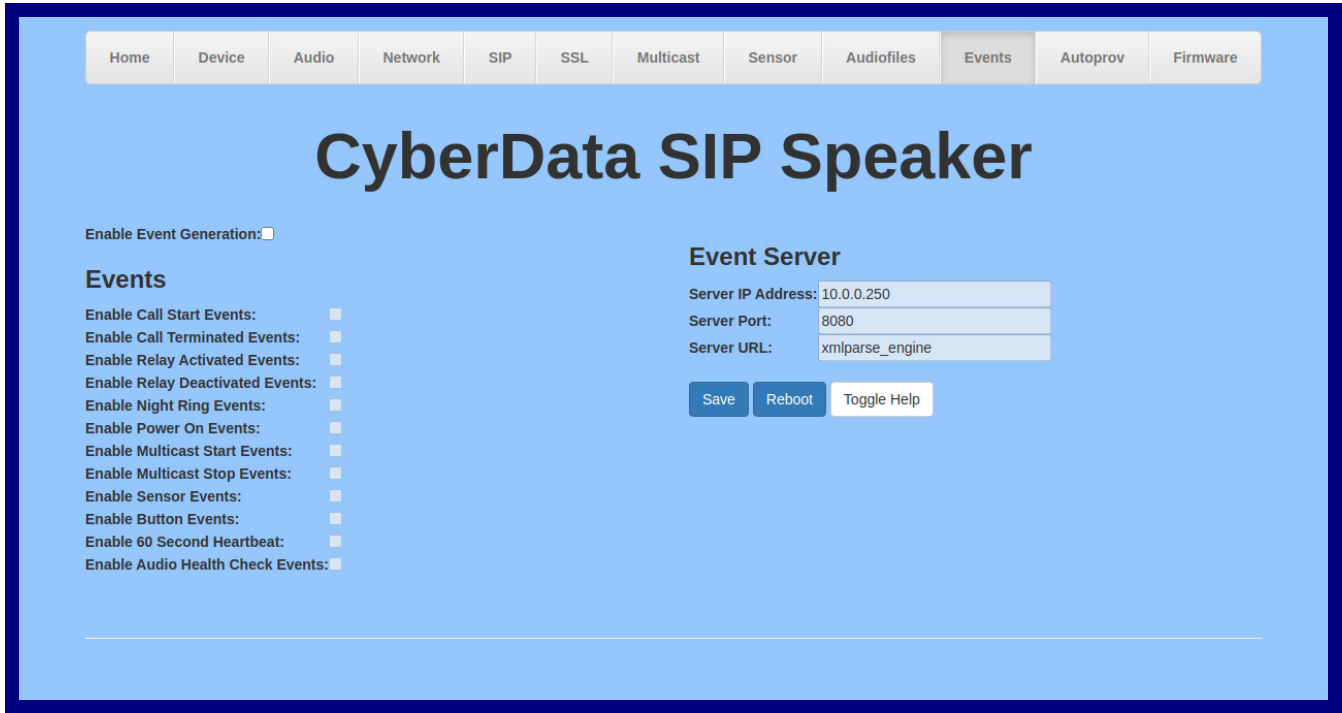
WAV (Microsoft) signed 16 bit PCM

2.3.13 Configure the Events Parameters

The **Events** page specifies a remote server that can be used to receive HTTP POST events when actions take place on the board.

1. Click on the **Events** menu button to open the **Events** page (Figure 2-31).

Figure 2-31. Event Configuration Page



2. On the **Events** page, enter values for the parameters indicated in [Table 2-15](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-15. Events Configuration Parameters

Web Page Item	Description
Enable Event Generation ?	The device will send HTTP POST events to the specified remote server and port number whenever a certain action takes place. Select an event type below to generate an HTTP POST event.
Events	
Enable Button Events ?	When selected, the device will report Call button presses.
Enable Call Start Events ?	When selected, the device will report the start of a SIP call.
Enable Call Terminated Events ?	When selected, the device will report the end of a SIP call.
Enable Relay Activated Events ?	When selected, the device will report relay activation.
Enable Relay Deactivated Events ?	When selected, the device will report relay deactivation.
Enable Night Ring Events ?	When selected, the device will report when it starts ringing upon an incoming SIP call to the Nightringer extension. As a reminder, the Nightringer extension always rings upon an incoming SIP call and it is not possible to alter this behavior.
Enable Power On Events ?	When selected, the device will report when it boots.
Enable Multicast Start Events ?	When selected, the device will report when the device starts playing a multicast audio stream.
Enable Multicast Stop Events ?	When selected, the device will report when the device stops playing a multicast audio stream.
Enable Sensor Events ?	When selected, the device will report when the on-board sensor is activated.
Enable 60 Second Heartbeat Events ?	When enabled, the device will report a Heartbeat event every 60 seconds. SIP registration is not required to generate Heartbeat events.
Enable Audio Health Check Events ?	When selected, the device will report the results of an audio health check.
Event Server	
Server IP Address ?	The IPv4 address of the event server in dotted decimal notation.
Server Port ?	Specify the event server port number. The supported range is 0-65536. Enter up to 5 digits.
Server URL ?	Generally, the destination URL is the name of the application that receives the events and the string in the HTTP POST command. It can be a script used to parse and process the HTTP POST events. Enter up to 127 characters.
Save	Click the Save button to save your configuration settings.
Reboot	Click on the Reboot button to reboot the system.
Toggle Help	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.13.1 Example Packets for Events

The server and port are used to point to the listening server and the 'Remote Event Server URL' is the destination URL (typically the script running on the remote server that's used to parse and process the POST events).

Note The XML is URL-encoded before transmission so the following examples are not completely accurate.

Here are example packets for every event:

```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData Device' MAC='0020f70015b6'>
<event>POWERON</event>
</cyberdata>
```

```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 199
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData Device' MAC='0020f70015b6'>
<event>HEARTBEAT</event>
</cyberdata>
```

```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 196
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData Device' MAC='0020f70015b6'>
<event>BUTTON</event>
</cyberdata>
```

```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 201
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData Device' MAC='0020f70015b6'>
<event>CALL_ACTIVE</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
```

```
User-Agent: CyberData/1.0.0
Content-Length: 205
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData Device' MAC='0020f70015b6'>
<event>CALL_TERMINATED</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData Device' MAC='0020f70015b6'>
<event>RINGING</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData Device' MAC='0020f70015b6'>
<event>MULTICAST_START</event>
<index>8</index>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 233
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData Device' MAC='0020f70015b6'>
<event>MULTICAST_STOP</event>
<index>8</index>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData Device' MAC='0020f70015b6'>
<event>RELAY_ACTIVATED</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
```

```
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData Device' MAC='0020f70015b6'>
<event>RELAY_DEACTIVATED</event>
</cyberdata>
```

```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData Device' MAC='0020f70015b6'>
<event>NIGHTRINGING</event>
</cyberdata>
```

2.3.14 Configure the Autoprovisioning Parameters

Autoprovisioning can be used to automatically configure your device. The autoprovisioning file is an xml file with the device configuration. Values found in this file will override values stored in on-board memory.

Note By default, the device will try to set up its configuration with autoprovisioning.

1. Click the **Autoprov** menu button to open the **Autoprovisioning** page. See [Figure 2-32](#).

Figure 2-32. Autoprovisioning Page

Home Device Audio Network SIP SSL Multicast Sensor Audiofiles Events **Autoprov** Firmware

CyberData SIP Speaker

Enable Autoprovisioning: ☒

Autoprovisioning Server:

Autoprovisioning Filename:

Use tftp: ☐

Verify Server Certificate: ☐

Username:

Password:

Autoprovisioning autoupdate (in minutes):

Autoprovision at time (HHMM):

Autoprovision when idle (in minutes > 10):

See the manual to learn how to use autoprovisioning to configure your device.

Autoprovisioning happens on boot.

The device will first look for a configured server address and filename.

If these haven't been configured, it will look for an autoprovisioning server in your list of DHCP options and try to download '0020f704fef6.xml' and if this fails, '000000cd.xml'.

Save Reboot Toggle Help

Download Template

Autoprovisioning log

```
2022-11-08 12:40:53 Autoprov: no autoprov triggers. Exiting...
2022-11-08 12:40:55 Autoprovisioning on boot
2022-11-08 12:40:56 Autoprov found server='http://10.0.0.242' in dhcp option 43
2022-11-08 12:40:56 Autoprov looking for 0020f704fef6.xml at http://10.0.0.242
2022-11-08 12:40:56 Autoprov downloading http://10.0.0.242/0020f704fef6.xml
2022-11-08 12:40:56 Got autoprov file. Parsing "0020f704fef6.xml"
2022-11-08 12:40:57 Autoprov: Processing ssl certificates
2022-11-08 12:40:57 No certificate elements in SSLCertificates
2022-11-08 12:40:57 Autoprov: Processing audio files
2022-11-08 12:40:57 Autoprov found server='10.0.1.118' in dhcp option 72
```


2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in [Table 2-16](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-16. Autoprovisioning Configuration Parameters





Web Page Item	Description
Enable Autoprovisioning ?	The device will automatically fetch a configuration file, also known as the 'autoprovisioning file', based on the configured settings below.
Autoprovisioning Server ?	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning Filename ?	<p>The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of <mac address>.xml.</p> <p>Supported filename extensions are .txt, and .xml. The current filename is denoted by an asterisk at the bottom of the Autoprovisioning Page. Enter up to 256 characters.</p> <p>A file may have any name with an xml extension. If a file name is entered, the device will look for the specified file name, and only that file.</p>
Use tftp ?	The device will use TFTP (instead of http) to download autoprovisioning files.
Verify Server Certificate ?	When using ssl to download autoprovisioning files, reject connections where the server address doesn't match the server certificate's common name.
Username ?	The username used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Password ?	The password used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Autoprovisioning Autoupdate (in minutes) ?	<p>The reoccurring time (in minutes) the device will wait before checking for new autoprovisioning files. Enter up to 6 digits. A value of 0 will disable this option.</p> <p>Note: To use the auto update options, enable the Enable NTP setting on the Device Configuration Page page (see Table 2-6).</p>
Autoprovision at time (HHMMSS) ?	<p>The time of day the device will check for a new autoprovisioning file. The time must be 6 characters in length and in HHMMSS format. An empty value will disable this option.</p> <p>Note: To use the auto update options, enable the Enable NTP setting on the Device Configuration Page page (see Table 2-6).</p>
Autoprovision when idle (in minutes > 10) ?	<p>The idle time (in minutes greater than 10) after which the device will check for a new autoprovisioning file. Enter up to 6 digits. A value of 0 will disable this option.</p> <p>Note: To use the auto update options, enable the Enable NTP setting on the Device Configuration Page page (see Table 2-6).</p>
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

Table 2-16. Autoprovisioning Configuration Parameters (continued)

Web Page Item	Description
	Press the Download Template button to create an autoprovisioning file for the device. See Section 2.3.14.3, "Download Template Button"
Autoprovisioning log	The autoprovisioning log provides information about the latest autoprovisioning attempt (i.e. dhcp options and server accessed and files parsed or not found).

2.3.14.1 Autoprovisioning

On boot, the device will look for an autoprovisioning server configured on the [Autoprovisioning Page](#) or specified as a DHCP option. When it finds a server, it will try to download the following (in order of preference):

1. The file configured on the autoprovisioning page.
2. A file named according to it's mac address (for example: 0020f7350058.xml).
3. The file 000000cd.xml

The file can be hosted using a standard web server (like apache, IIS, or nginx), and the device can download over SSL. The file server can be an ipv4 address in dotted decimal notation or a fully qualified domain name.

By default, the device will get its autoprovisioning server from the DHCP options. See [Section 2.3.14.2, "Sample dhcpd.conf"](#) for an example of how to configure dhcpd to offer autoprovisioning server addresses. If multiple options are set, the device will attempt to download autoprovisioning files from every server.

The DHCP option determines the protocol used to download the autoprovisioning file. The device looks for DHCP options in the following order:

1. Option 43 - a FQDN or an IP address to an http server
2. Option 72 - an IP address to an http server
3. Option 150 - an IP address to a tftp server
4. Option 66 - an IP address to a tftp server or if the entry starts with 'http', a FQDN to a http server.

You can download an autoprovisioning template file from the [Autoprovisioning Page](#) using the **Download Template** button (see [Table 2-16](#)). This file contains every configuration option that can be set on the board.

Autoprovisioning files can contain the whole configuration or a subset of this file. The first autoprovisioning file can also contain links to other autoprovisioning files.

The <MiscSettings> section contains some examples of additional autoprovisioning files:

```
<MiscSettings>
    <DeviceName>CyberData Device</DeviceName>
<!--    <AutoprovFile>common.xml</AutoprovFile>-->
<!--    <AutoprovFile>sip_reg[macaddress].xml</AutoprovFile>-->
<!--    <AutoprovFile>audio[macaddress]</AutoprovFile>-->
<!--    <AutoprovFile>device[macaddress].xml</AutoprovFile>-->
</MiscSettings>
```

After downloading the first autoprovisioning file, the device will step through up to twenty additional <AutoprovFile> entries and try to download these files from the same server.

When the device finds a filename with the string **[macaddress]**, it will replace this string with the mac address.

As an example, the user has configured option 43 on their DHCP server to "http://example.com," and on their server, they have a file named **0020f7123456.xml** (the same as the mac address of the device).

The file 0020f7123456.xml contains:

```
<?xml version="1.0" encoding="utf-8" ?>
<specific>
  <MiscSettings>
    <DeviceName>Newname</DeviceName>
    <AutoprovFile>common.xml</AutoprovFile>
    <AutoprovFile>sip_reg[macaddress].xml</AutoprovFile>
    <AutoprovFile>audio[macaddress]</AutoprovFile>
    <AutoprovFile>device.xml</AutoprovFile>
  </MiscSettings>
</specific>
```

1. The device will first set it's name to 'Newname'.
2. It will try to download http://example.com/common.xml.
3. It will try to download http://example.com/sip_reg0020f7123456.xml.
4. It will try to download http://example.com/audio0020f7123456.
5. It will try to download http://example.com/device.xml.

The device is reconfigured every time it downloads a new file so if two files configure the same option the last one will be the one that is saved.

It is possible to autoprovision autoprovisioning values (for example, to disable autoprovisioning or to configure a time to check for new files).

Checking for New Autoprovisioning Files after Boot

The device will always check for an autoprovisioning files on boot but it can be configured to also check after a periodic delay, when idle, or at a specified time. When one of these options is set, the device will download its autoprovisioning files again, and if it finds any differences from the files it downloaded on boot, it will force a reboot and reconfigure.

The
Autoprovisioning
Filename

The autoprovisioning filename can contain a file, a file path, or a directory.

Table 2-17. Autoprovisioning File Name

Autoprovisioning Filename	Autoprovisioning Server	File Downloaded
config.xml	10.0.1.3	10.0.1.3/config.xml
/path/to/config.xml	10.0.1.3	10.0.1.3/path/to/config.xml
subdirectory/path/	10.0.1.3	10.0.1.3/subdirectory/path/0020f7020002.xml

TFTP options may not support subdirectories. If a directory is set in the filename field, firmware and audio files will also be downloaded from this subdirectory.

If the filename ends with a forward slash “/,” the device will treat it as a subdirectory.

For example:

The autoprovisioning server is set to “https://www.example.com”

The autoprovisioning filename is set to “cyberdata/”

On boot, the device will try to download:

https://www.example.com/cyberdata/0020f7123456.xml

...and if this fails:

https://www.example.com/cyberdata/000000cd.xml

Audio files and firmware files will also add “cyberdata” to the URL before downloading.

```

Autoprovisioning <FirmwareSettings>
Firmware Updates <FirmwareFile>505-ulmage-ceilingsspeaker</FirmwareFile>
                  <FirmwareServer>10.0.1.3</FirmwareServer>
                  <OutdoorIntercom30>firmware_file_v9.3.0</OutdoorIntercom30>
                  <OutdoorIntercom31>firmware_file_v10.3.0</OutdoorIntercom31>
                  <CallButton31>firmware_file_v10.3.0</CallButton31>
                  </FirmwareSettings>

```

In the <FirmwareSettings> section, the <FirmwareServer> element can be used to specify a different server for hosting firmware files. When this element is not available, the device will try to download the file from the autoprovisioning server.

The device will use the filename to determine when to autoprovision firmware updates. The default configuration is blank, so the first time you set a value in your autoprovisioning file, it may force a firmware update even if the firmware version has not changed.

The <FirmwareFile> name can contain path elements (i.e. /path/to/firmware/10.3.0-ulmage-[device_file_name]).

The device also supports product strings for downloading firmware. If the <FirmwareFile> option is not set, the device will look for its particular product string for a firmware filename. In this way, a generic autoprovisioning file can specify unique firmware for a range of products.

The list of valid product strings:

```

<ProductString>CallButton31</ProductString>
<ProductString>EmergencyIntercom31</ProductString>
<ProductString>EmergencyIntercom31SW</ProductString>
<ProductString>IndoorIntercom31</ProductString>
<ProductString>IndoorIntercom31SW</ProductString>
<ProductString>IndoorKeypad31</ProductString>
<ProductString>IndoorKeypad31SW</ProductString>
<ProductString>OfficeRinger31</ProductString>
<ProductString>OfficeRinger31SW</ProductString>
<ProductString>OutdoorIntercom31</ProductString>
<ProductString>OutdoorIntercom31SW</ProductString>
<ProductString>OutdoorKeypad31</ProductString>
<ProductString>OutdoorKeypad31SW</ProductString>
<ProductString>Strobe31</ProductString>
<ProductString>Strobe31SW</ProductString>

```

Autoprovisioning
Example 1

Here's a simple example using four autoprovisioning files to configure two devices:

We boot up two devices with mac addresses **00:20:f7:02:00:01** and **00:20:f7:02:00:02** (Device1 and Device2).

The devices are set to use DHCP and that server provides an autoprovisioning server address with option 43. The address is “https://autoprovtest.server.net.” The files on this server are as follows:

000000cd.xml

```
<MiscSettings>
<DeviceName>CyberData Autoprovisioned</DeviceName>
<AutoprovFile>sip_common.xml</AutoprovFile>
<AutoprovFile>sip_[macaddress].xml</AutoprovFile>
</MiscSettings>
```

sip_common.xml

```
<SIPSettings>
<SIPServer>10.0.0.253</SIPServer>
<RemoteSIPPort>5060</RemoteSIPPort>
</SIPSettings>
```

sip_0020f7020001.xml

```
<SIPSettings>
<SIPUserID>198</SIPUserID>
<SIPAuthPassword>ext198</SIPAuthPassword>
<DialoutExtension0>204</DialoutExtension0>
</SIPSettings>
```

sip_0020f7020002.xml

```
<SIPSettings>
<SIPUserID>500</SIPUserID>
<SIPAuthPassword>ext500</SIPAuthPassword>
<DialoutExtension0>555</DialoutExtension0>
</SIPSettings>
```

On boot, Device1 tries to fetch the file **0020f7023614.xml** from “https://autoprovtest.server.net”. This file is not available, so device1 then tries to fetch the file **000000cd.xml**. This file exists, and Device1 parses the three elements.

1. Device1 changes its device name to **CyberData Autoprovisioned**.
2. Device1 finds an AutoprovFile element containing the filename **sip_common.xml**. The device downloads **sip_common.xml** from “https://autoprovtest.server.net,” and imports this configuration, setting the sip server to **10.0.0.253** and the remote port to **5060.3**.
3. Device1 finds another AutoprovFile element containing the filename **sip_[macaddress].xml**. The device replaces the **[macaddress]** with its own mac address value creating **sip_0020f7020001.xml**, downloads this file from “https://autoprovtest.server.net,” and imports this configuration. This sets the user ID to **198**, the password to **ext198**, and the dialout extension to **204**. Device1 is now finished with autoprovisioning.

Device2 goes through the same steps by setting its device name to **CyberData Autoprovisioned**, its SIP server to **10.0.0.253**, and its port to **5060**. When Device2 “sees” **sip_[macaddress].xml**, Device2 replaces it with its own mac address and downloads **sip_0020f7020002.xml** from “https://autoprovtest.server.net.” Device2 sets the SIP User ID to **500**, the password to **ext500**, and the dialout extension to **555**.

Autoprovisioning Example 2

Here is another example of setting up your autoprovisioning files:

We boot up two devices with mac addresses **00:20:f7:02:00:01** and **00:20:f7:02:00:02** (Device1 and Device2) and boot them on a network with a DHCP server configured with an autoprovisioning server at **10.0.1.3** on option **150**. Our TFTP server has three files:

0020f7020001.xml

```
<MiscSettings>
<AutoprovFile>common_settings.xml</AutoprovFile>
</MiscSettings>
<SIPSettings>
<SIPUserID>198</SIPUserID>
<SIPAuthPassword>ext198</SIPAuthPassword>
<DialoutExtension0>204</DialoutExtension0>
</SIPSettings>
```

0020f7020002.xml

```
<MiscSettings>
<AutoprovFile>common_settings.xml</AutoprovFile>
</MiscSettings>
<SIPSettings>
<SIPUserID>500</SIPUserID>
<SIPAuthPassword>ext500</SIPAuthPassword>
<DialoutExtension0>555</DialoutExtension0>
</SIPSettings>
```

common_settings.xml

```
<MiscSettings>
<DeviceName>CyberData Autoprovisioned</DeviceName>
</MiscSettings>
<SIPSettings> <SIPServer>10.0.0.253</SIPServer>
<RemoteSIPPort>5060</RemoteSIPPort>
</SIPSettings>
```

1. On boot, Device1 downloads **0020f7020001.xml** from **10.0.1.3** and imports these values. The SIP User ID is **198**, the password is **ext198**, and the dialout extension is **204**.

2. Device1 then gets the filename **common_settings.xml** from the AutoprovFile element and downloads this file from the TFTP server at **10.0.1.3**. and imports these settings. The device name is set to **CyberData Autoprovisioned**, the SIP server is set to **10.0.0.253**, and the port is set to **5060**.

Device2 does the same except it downloads **0020f7020002.xml** on boot and imports these values instead. The Sip User ID is **500**, password is **ext500**, and dialout extension is **555**. Device2 then downloads the **common_settings.xml** file and imports those values. The device name is set to **CyberData Autoprovisioned**, the SIP server is set to **10.0.0.253**, and the port is set to **5060**.

XML Files

XML files can contain <AutoprovFile> elements. If multiple DHCP options are specified, the device will try to download autoprovisioning files from each in turn. The device will only look for <AutoprovFile> elements in the first file downloaded from each server. You can specify up to 20 <AutoprovFile> elements in the first autoprovisioning file.

There are numerous ways to change an element of the **configuration(xml)** file. Using **sip ext** as an example, the extension can be changed:

Within the device-specific xml, i.e. **[macaddress].xml**, via the AutoprovFile element:<SIPSettings>/<SIPExt>

From the device specific xml, a pointer to a sip_common file

From the device specific xml, a pointer to the device specific sip_[macaddress].xml

From the common file, a pointer to sip_common.xml

From the common file, a pointer to the device specific (sip_[macaddress].xml)

Autoprovisioned Audio Files

Audio files are stored in non-volatile memory and an autoprovisioned audio file will only have to be downloaded once for each device. Loading many audio files to the device from the web page could cause it to appear unresponsive. If this happens, wait until the transfer is complete and then refresh the page.

The device uses the file name to determine when to download a new audio file. This means that if you used autoprovisioning to upload a file and then changed the contents of this file at the TFTP server, the device will not recognize that the file has changed (because the file name is the same).

Since audio files are stored in non-volatile memory, if autoprovisioning is disabled after they have been loaded to the board, the audio file settings will not change. You can force a change to the audio files on the board by clicking **Restore Default** on the **Audio Configuration** page or by changing the autoprovisioning file with “**default**” set as the file name.

2.3.14.2 Sample dhcpd.conf

```

#
# Sample configuration file for ISC dhcpd for Debian
#

ddns-update-style none;

option domain-name "voiplab";
option domain-name-servers 10.0.0.252;
option option-150 code 150 = ip-address;
option ntp-servers north-america.pool.ntp.org;
option space VendorInfo;
option VendorInfo.text code 10 = { text };
authoritative;
log-facility local7;

subnet 10.0.0.0 netmask 255.0.0.0 {
    max-lease-time 3600;
    default-lease-time 3600;

    option routers                10.0.0.1;
    option subnet-mask            255.0.0.0;

    option domain-name            "voiplab";
    option domain-name-servers    10.0.0.252;

    option time-offset            -8;                # Pacific Standard Time

#    option www-server            99.99.99.99;        # OPTION 72

#    option tftp-server-name      "10.0.1.52";        # OPTION 66
#    option tftp-server-name      "http://test.cyberdata.net"; # OPTION 66

#    option option-150            10.0.0.252;        # OPTION 150

# These two lines are needed for option 43
#    vendor-option-space VendorInfo;                # OPTION 43
#    option VendorInfo.text "http://test.cyberdata.net"; # OPTION 43

    range 10.10.0.1 10.10.2.1; }

```

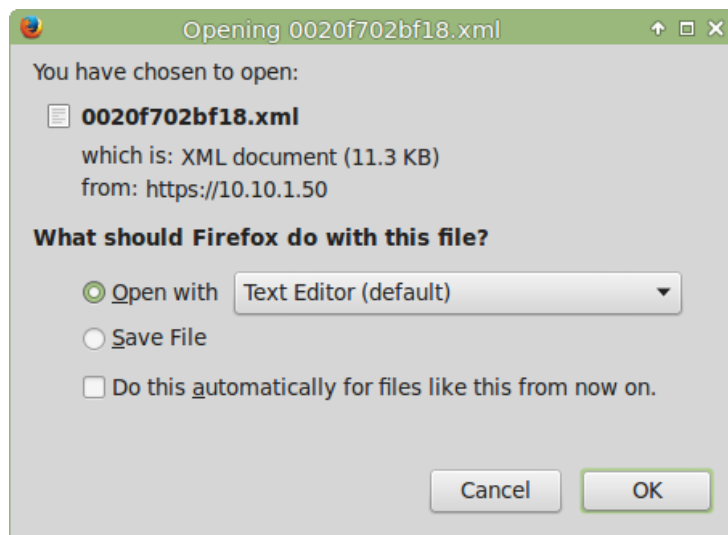
2.3.14.3 Download Template Button

The **Download Template** button allows the user to generate, download, edit, and then store an autoprovisioning template on the server that serves the autoprovisioning files for devices.

To generate an autoprovisioning template directly from the device, complete the following steps:

1. On the **Autoprovisioning** page, click on the **Download Template** button.
2. You will see a window prompting you to save a configuration file (**.xml**) to a location on your computer ([Figure 2-33](#)). The configuration file is the basis for the default configuration settings for your unit).
3. Choose a location to save the configuration file and click on **OK**. See [Figure 2-33](#).

Figure 2-33. Configuration File



4. At this point, you can open and edit the autoprovisioning template to change the configuration settings in the template for the unit.
5. You can then upload the autoprovisioning file to a TFTP or HTTP server where the file can be loaded onto other devices.

2.4 Upgrade the Firmware and Reboot the SIP Speaker with Talk-Back

2.4.1 Downloading the Firmware

To download the firmware to your computer:

1. Download the latest firmware file from the **Downloads** tab at the following webpage:
<https://www.cyberdata.net/products/011394>
2. Unzip the firmware version file. This file may contain the following:
 - Firmware file
 - Release notes
 - Autoprovisioning template
3. Log in to the **Home** page as instructed in [Section 2.3.4, "Log in to the Configuration Home Page"](#).
4. Click on the **Firmware** menu button to open the **Firmware** page ([Figure 2-34](#)).

Note CyberData strongly recommends that you do not upgrade the firmware when the device is likely to be in use.

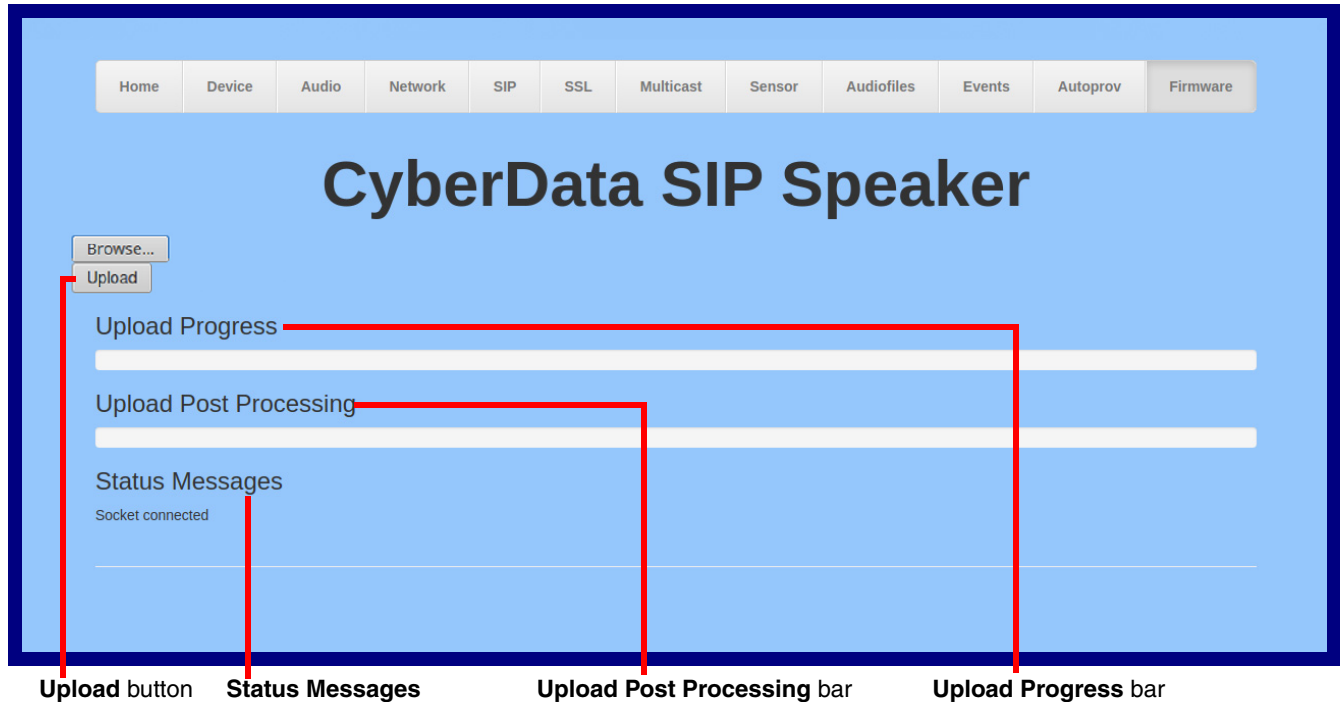
Figure 2-34. Firmware Page



5. Click on the **Browse** button, and then navigate to the location of the firmware file.

6. Select the firmware file. This reveals the **Upload** button (Figure 2-35).

Figure 2-35. Upload Button



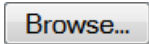

7. Click on the **Upload** button. After selecting the **Upload** button, you will see the progress of the upload in the **Upload Progress** bar.
8. When the upload is complete, you will see the words **Upload finished** under **Status Messages**.
9. At this point, you will see the progress of the upload's post processing in the **Upload Post Processing** bar.

Note Do not reboot the device before the upgrading process is complete.

10. When the process is complete, you will see the words **SWUPDATE Successful** under **Status Messages**.
11. The device will reboot automatically.
12. The **Home** page will display the version number of the firmware and indicate which boot partition is active.

Table 2-18 shows the web page items on the **Firmware** page.

Table 2-18. Firmware Page Parameters

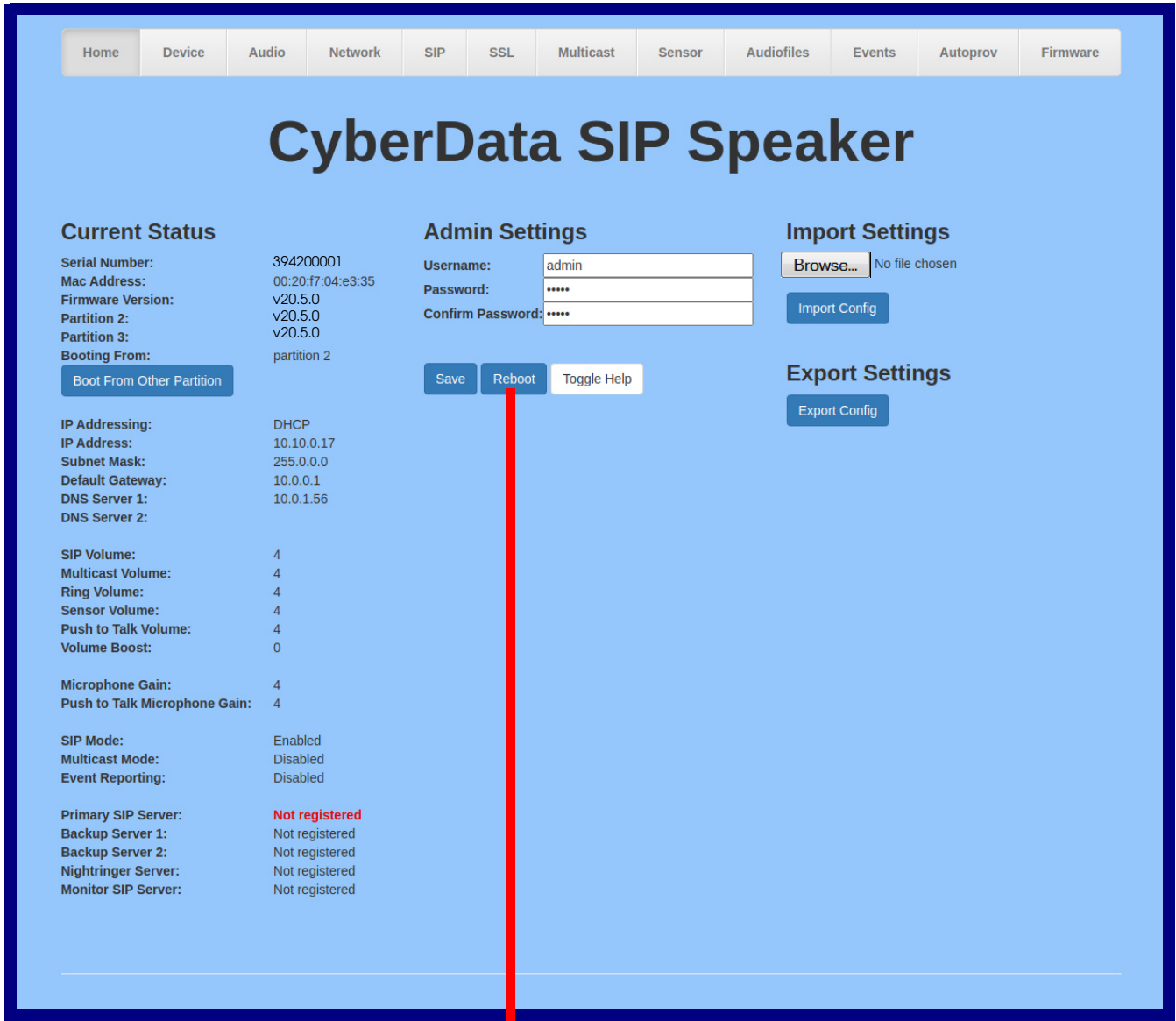
Web Page Item	Description
	Use the Browse button to navigate to the location of the firmware file that you want to upload.
	Click on the Upload button to automatically upload the selected firmware and reboot the system. Note: This button only appears after the user has selected a firmware file.
Upload progress	Status bar indicates the progress in uploading the file.
Upload Post Processing	Status bar indicates the progress of the software installation.
Status Messages	Messages relevant to the firmware update process appear here.

2.4.2 Reboot the Device

To reboot a SIP Speaker with Talk-Back, log in to the web page as instructed in [Section 2.3.4, "Log in to the Configuration Home Page"](#).

1. Click on the **Reboot** button on the **Home** page ([Figure 2-36](#)). A normal restart will occur.

Figure 2-36. Home Page



Reboot

2.5 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in [Table 2-19](#) use the free unix utility, **wget**, but any program that can send http POST commands to the device should work.

2.5.1 Command Interface Post Commands

These commands require an authenticated session (a valid username and password to work).

Table 2-19. Command Interface Post Commands

Device Action	HTTP Post Command ^a
Reboot	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=reboot"
Place call to extension (example: extension 600)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=call&extension=600"
Terminate a call	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=terminate"
Speak IP Address	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=speak_ip_address"
Test Audio	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=test_audio"
Swap Boot partitions	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.10.1.81/command" --post-data "request=swap_boot_partition"

^a.Type and enter all of each http POST command on one line.

Appendix A: Mounting the Speaker

A.1 Ceiling Tile Mounting

Before you mount the speaker, make sure that you have received all the parts for each speaker. Refer to [Table A-1](#) and [Table A-2](#).

Table A-1. Drop Ceiling Mounting Components (Part of the Accessory Kit)



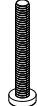

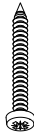
Quantity	Part Name	Illustration
3	#8 Nylon Thumb Nuts	
3	#8 Fender Washers	
3	8-32 x 1 1/4" Mounting Screws	

Table A-2. Drywall Mounting Components (Part of the Accessory Kit)

Quantity	Part Name	Illustration
3	Plastic Ribbed Anchors	
3	#8 Sheet Metal Screws	

To mount the speaker:

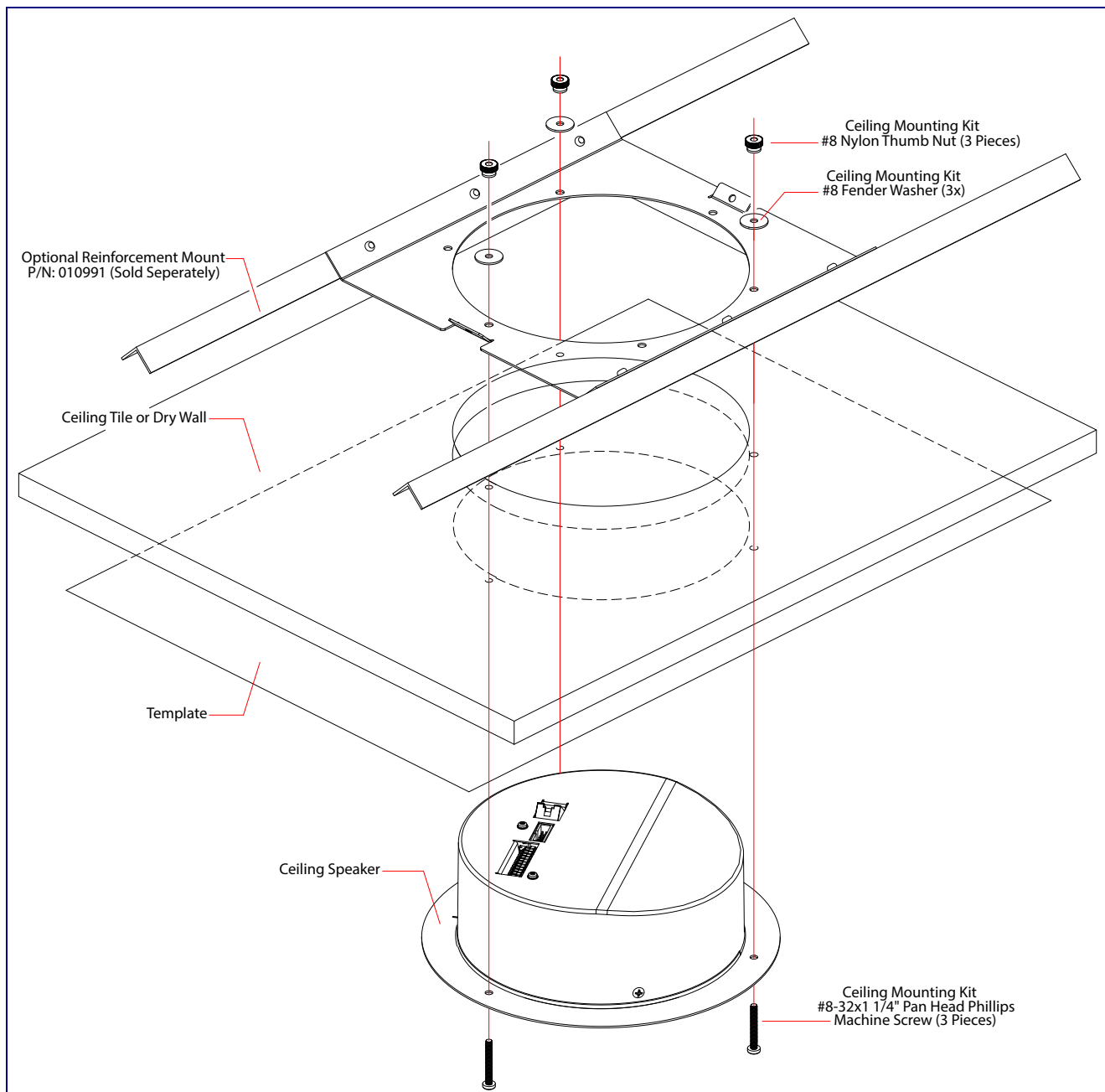
1. Use the **TEMPLATE** to cut the speaker hole and prepare holes for the screws ([Figure A-1](#)). This template is located on the back page of the *Installation Quick Reference Guide* that is delivered with each speaker.
2. Plug the Ethernet cable into the Speaker Assembly. [Section 2.2.3, "Confirm that the Speaker is Operational and Linked to the Network"](#) explains how the **Link** and **Status** LEDs work.
3. At this point:
 - For *drop ceiling mounting*, position the **IP SPEAKER ASSEMBLY** in the ceiling so that its screw holes align with those you prepared.
 - For *drywall mounting*, place the three **PLASTIC RIBBED ANCHORS** in the holes you prepared, and position the **IP SPEAKER ASSEMBLY** over them, aligning the screw holes in the assembly with the anchors.
4. To fasten the speaker:
 - For *drop ceiling mounting*, use the three **8-32 x 1 1/4" MOUNTING SCREWS**, **#8 NYLON THUMB NUTS**, and **#8 FENDER WASHERS** to secure the speaker.

Note For weak ceiling tile, CyberData offers a reinforcing mount (CyberData part number 010991A).

- For *drywall mounting*, use the three **#8 SHEET METAL SCREWS** to secure the speaker.

* For weak ceiling tile, CyberData offers a reinforcing mount (CyberData part number 010991).

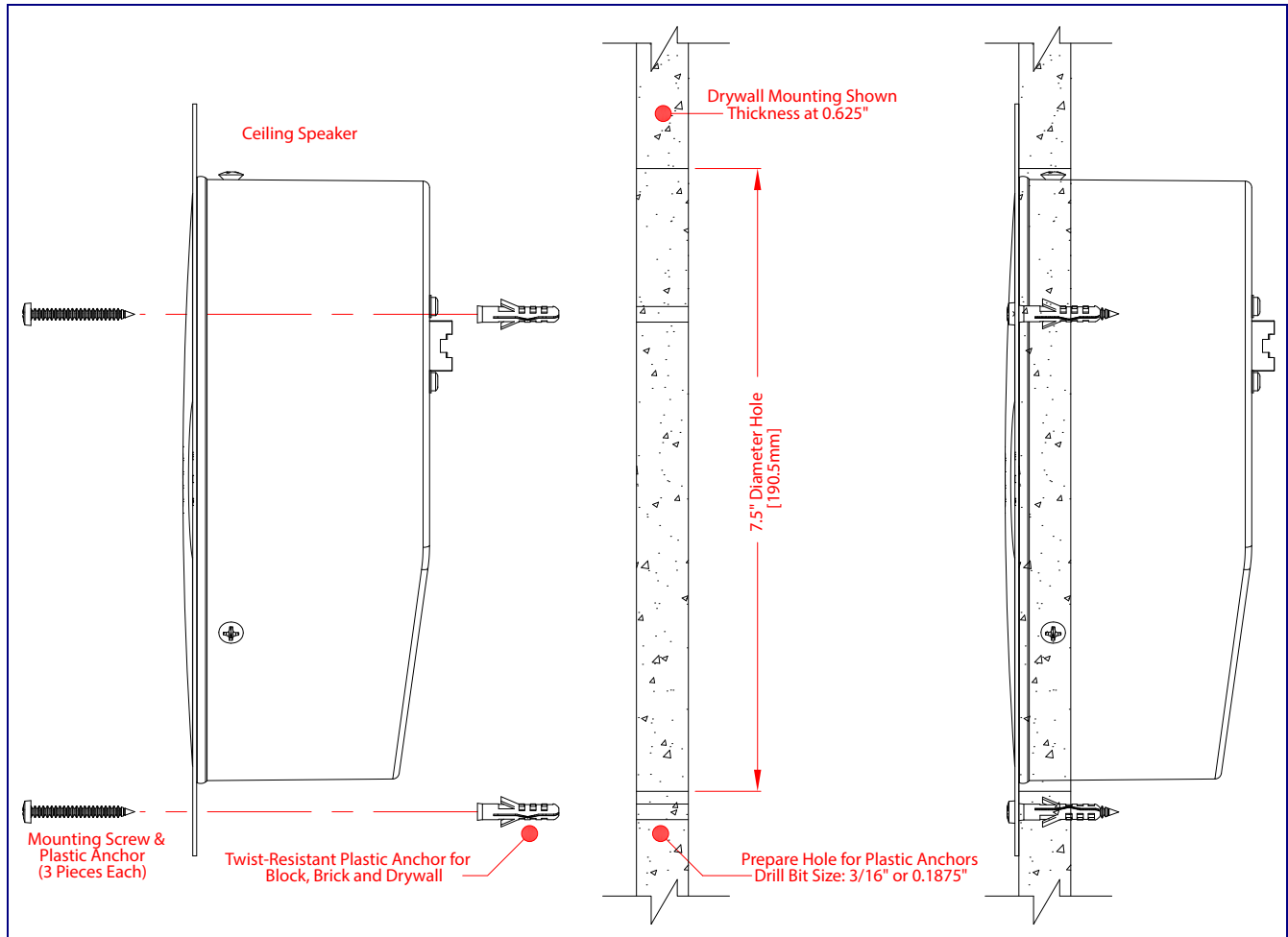
Figure A-1. Ceiling Tile Mounting



A.2 Drywall Mounting

Figure A-3 shows the drywall mounting for the SIP Speaker with Talk-Back.

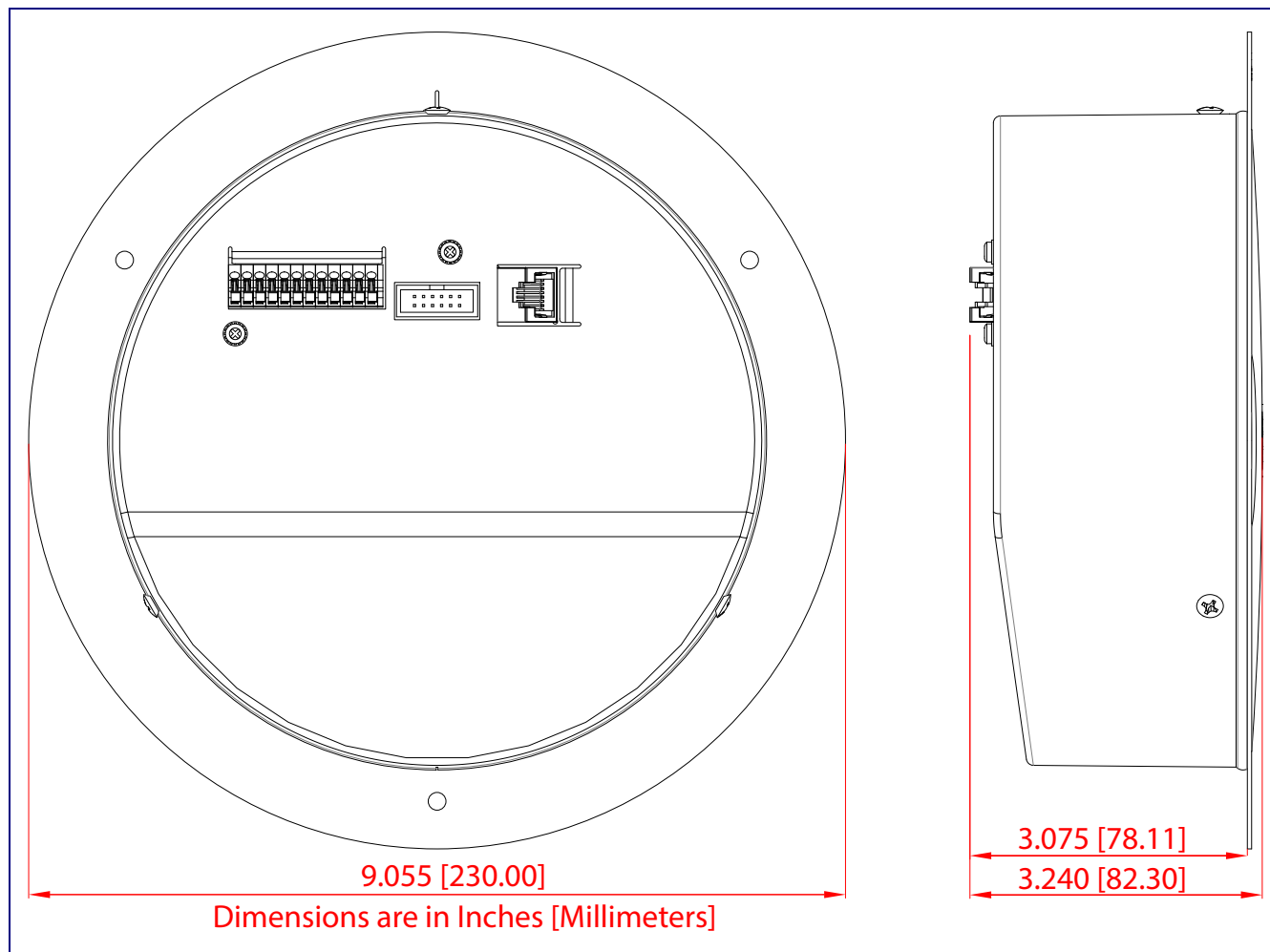
Figure A-2. Drywall Mounting



A.3 Dimensions

Figure A-3 shows the dimensions for the SIP Speaker with Talk-Back.

Figure A-3. Dimensions



Appendix B: Troubleshooting/Technical Support

B.1 Frequently Asked Questions (FAQ)

To see a list of frequently asked questions for your product, click on the **FAQs** tab at the following webpage:

<https://www.cyberdata.net/products/011394>

B.2 Documentation

The documentation for this product is released in an English language version only.

To download PDF copies of CyberData product documentation, click on the following webpage:

<https://www.cyberdata.net/products/011394>

B.3 Contact Information

Contact	<p>CyberData Corporation 3 Justin Court Monterey, CA 93940 USA www.cyberdata.net Phone: 800-CYBERDATA (800-292-3732) Fax: 831-373-4193</p>
Sales	<p>Sales 831-373-2601, Extension 334</p>
Technical Support	<p>The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:</p> <p>https://support.cyberdata.net/</p> <p>The Support Form initiates a ticket which CyberData uses for tracking customer requests. Most importantly, the Support Form tells us which PBX system and software version that you are using, the make and model of the switch, and other important information. This information is essential for troubleshooting. Please also include as much detail as possible in the Comments section of the Support Form.</p> <p>Phone: (831) 373-2601, Extension 333</p>

B.4 Warranty and RMA Information

The most recent warranty and RMA information is available at the following website address:

<https://support.cyberdata.net/>

Index

Symbols

#8 fender washers 89, 90
 #8 nylon thumb nuts 89, 90
 #8 sheet metal screws 89, 90

Numerics

8-32 x 1 1/4" mounting screws 89, 90

A

address, configuration login 23
 adjusting volume 18
 announcing a speaker's IP address 17, 18
 audio configuration 62
 night ring tone parameter 64
 audio files, user-created 66
 audio output 5
 audio page 62
 audio test 17, 18
 autoprovision at time (HHMMSS) 74
 autoprovision when idle (in minutes > 10) 74
 autoprovisioning 75
 download template button 75
 autoprovisioning autoupdate (in minutes) 74
 autoprovisioning configuration 73, 74
 autoprovisioning filename 74
 autoprovisioning server (IP Address) 74

B

backup SIP server 1 40
 backup SIP server 2 40
 backup SIP servers, SIP server
 backups 40
 boost (volume) 32

C

changing
 the web access password 27
 Cisco SRST 42
 command interface 88

commands 88
 configurable parameters 28, 32, 36, 40
 configuration
 audio 62
 default IP settings 19
 device 9
 door sensor 48, 57
 intrusion sensor 48, 57
 network 35
 SIP 38
 configuration home page 23
 configuration page
 configurable parameters 28, 32, 36
 confirming IP address 17, 18
 contact information 95
 contact information for CyberData 95
 current network settings 36
 CyberData contact information 95

D

default
 web login username and password 23
 default gateway 36
 default IP settings 19
 default login address 23
 device configuration 9, 27
 device configuration parameters 74
 the device configuration page 73
 device configuration page 27, 31
 device configuration parameters 28, 32
 device configuration password
 changing for web configuration access 27
 dial out extension (door sensor) 59
 dial out extension strings 45
 dial-out extension strings 47
 dimensions 5, 6
 discovery utility program 23
 DNS server 36
 door sensor 57, 64
 dial out extension 59
 door sensor normally closed 59
 play audio locally 59
 download autoprovisioning template button 75
 drop ceiling mounting of speaker 90
 drywall mounting of speaker 90
 DTMF
 monitor DTMF toggle key 29, 32
 DTMF tones 47
 DTMF tones (using rfc2833) 45

E

- enable night ring events 69
- Ethernet cable 90
- event configuration
 - enable night ring events 69
- expiration time for SIP server lease 40, 41, 44
- export settings 25

F

- factory default settings
 - how to set 18
- features 3
- firmware
 - where to get the latest firmware 84

G

- get autoprovisioning template 75

H

- home page 23
- http POST command 88

I

- identifying your product 1
- illustration of speaker mounting process 89
- import settings 25
- import/export settings 25
- installation, typical speaker system 2
- intrusion sensor 57
- IP address 36

L

- lease, SIP server expiration time 40, 41, 44
- lengthy pages 56
- link LED 90
- local SIP port 41
- log in address 23

M

- MGROUP
 - MGROUP Name 55
- monitor authenticate ID 41
- monitor authenticate password 41
- monitor DTMF toggle key 29, 32
- monitor user ID 41
- mounting a speaker 89
- multicast configuration 54, 62
- Multicast IP Address 55

N

- navigation (web page) 20
- navigation table 20
- network configuration 35
- network link activity, verifying 16
- nightring tones 56
- Nightringer 83
- nightringer settings 43
- NTP server 28

O

- overview 1

P

- pages (lengthy) 56
- parts
 - #8 fender washers 89
 - #8 nylon thumb nuts 89
 - #8 sheet metal screws 89
 - 8-32 x 1 1/4" mounting screws 89
 - plastic ribbed anchors 89
- password
 - for SIP server login 40
 - login 23
- payload types 5
- plastic ribbed anchors 89, 90
- play audio locally (door sensor) 59
- point-to-point configuration 46
- polycom default channel 56
- polycom emergency channel 56
- polycom priority channel 56
- port
 - local SIP 41
 - remote SIP 41
- POST command 88

- power input (J1) 5
- power requirement 5
- power, connecting to speaker 10
- priority
 - assigning 56
- product
 - mounting 89
 - parts list 8
- product features 3
- product overview 1
 - product features 3
 - product specifications 5
- product specifications 5

R

- reboot 86, 87
- remote SIP port 41
- Reset Test Function Management (RTFM) button 17, 18
- restoring the factory default settings 18
- ringtones 56
 - lengthy pages 56
- rport discovery setting, disabling 42
- RTFM button 17, 18

S

- sales 95
- sensor
 - sensor normally closed 59
 - sensor timeout 59
- sensor setup page 48, 58
- sensor setup parameters 48, 57
- sensors 59
- server address, SIP 40
- service 95
- SIP
 - enable SIP operation 40, 41
 - local SIP port 41
 - user ID 40
- SIP configuration 38
- SIP configuration parameters
 - outbound proxy 41, 44
 - registration and expiration, SIP server lease 40, 41, 44
 - user ID, SIP 40
- SIP registration 40
- SIP remote SIP port 41
- SIP server 40
 - password for login 40
 - user ID for login 40
- SIP server configuration 40

- SIP volume 32
- SRST 42
- status LED 90
- subnet mask 36

T

- tech support 95
- technical support, contact information 95
- template for speaker and screw holes 90
- testing audio 17, 18
- typical system installation 2

U

- user ID
 - for SIP server login 40
- username
 - changing for web configuration access 27
 - default for web configuration access 23

V

- verifying
 - network link and activity 16
 - power on to speaker 16
- VLAN ID 36
- VLAN Priority 36
- VLAN tagging support 36
- VLAN tags 36
- volume
 - multicast volume 32
 - ring volume 32
 - sensor volume 32
 - SIP volume 32
- volume boost 32
- volume, adjusting 18

W

- warranty policy at CyberData 95
- web configuration log in address 23
- web page
 - navigation 20
- web page navigation 20
- weight 5
- wget, free unix utility 88